DIAGNOSTICO Y MEJORAS DE LA SITUACIÓN ACTUAL AL PROCESO: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD AUTÓNOMA DE OCCIDENTE

KAREN DAJANA PERAFÁN MONTENEGRO

UNIVERSIDAD AUTÓNOMA DE OCCIDENTE
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE OPERACIONES Y SISTEMAS
PROGRAMA DE INGENIERÍA INFORMÁTICA
SANTIAGO DE CALI
2015

DIAGNOSTICO Y MEJORAS DE LA SITUACIÓN ACTUAL AL PROCESO: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD AUTÓNOMA DE OCCIDENTE

KAREN DAJANA PERAFÁN MONTENEGRO

Proyecto de grado para optar al título de Ingeniero en Informática

Director
MARIO WILSON CASTRO TORRES
Ingeniero en Sistemas

UNIVERSIDAD AUTÓNOMA DE OCCIDENTE
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE OPERACIONES Y SISTEMAS
PROGRAMA DE INGENIERÍA INFORMÁTICA
SANTIAGO DE CALI
2015

Nota de aceptación:

Aprobado por el Comité de Grado en cumplimiento de los requisitos exigidos por la Universidad Autónoma de Occidente para optar al Título de ingeniero en informática

LYDA PEÑA PAZ

_____

Jurado

MIGUEL JOSE NAVAS JAIME

_____

Jurado

Santiago de Cali, 9 de Enero de 2015

Dedicado con todo el amor a mis padres y a las personas que han estado durante este proceso de formación profesional y personal, gracias por el apoyo incondicional, al gran esfuerzo de mis padres por luchar juntos para cumplir mis metas y sueños. A mi padre por ser el ejemplo de superación, estudio y progreso a seguir que inculcó en mí. Padres, hermanos, sobrinos, tías, amigos gracias por todo.

AGRADECIMIENTOS

A Dios por darme el privilegio de la vida y haber permitido iniciar y culminar una carrera profesional.

Al Ingeniero Mario Wilson Castro, por su apoyo y dirección durante el proyecto desarrollado.

Al Ingeniero Jorge Armando Rojas, por el acompañamiento y enseñanza profesional para el progreso del desarrollo del proyecto.

A Maira Alejandra Castañeda por su acompañamiento y apoyo moral en la elaboración del proyecto.

A Jonathan David Bonilla por su acompañamiento y apoyo durante toda la formación profesional.

CONTENIDO

Pág.

LISTADO DE TABLAS

Pág.

LISTADO DE FIGURAS

Pág.

LISTADO DE ANEXOS

Pág.

RESUMEN

Actualmente el activo más importante para una organización es la información, por ende esta merece un cuidado y seguimiento para la continuidad y supervivencia del negocio. La Universidad Autónoma de Occidente a partir de esto ha adquirido un rol y compromiso con la seguridad de la información en su comunidad universitaria, adoptando medidas para la mitigación de riesgos dentro y fuera de sus instalaciones.

Uno de los mecanismos a seguir para la verificación a la gestión de la seguridad y privacidad de la información es la realización de auditorías para la identificación del uso adecuado de la información y de los recursos tecnológicos; el siguiente documento describe como realizar una gestión a un programa de auditoria interna de seguridad y privacidad de la información en la Universidad Autónoma de Occidente.

Como guía base se usan las normas ISO/IEC 27001:2013 Sistema de gestión de seguridad de la información, ISO/IEC 27002:2013 Código de práctica para la gestión de la seguridad de la información y la ISO19011:2012 Directrices para la auditoria de los sistemas de gestión. A través de estas normas se definen lineamientos, directrices, políticas, normas, procedimientos y formatos para la realización de auditorías en seguridad y privacidad de la información, además se orienta que la actividad vaya a la oportunidad de mejora al proceso en torno a la seguridad y privacidad de la información como a la concienciación del tema en toda la comunidad universitaria.

Palabras clave: seguridad de la información, seguridad informática, auditoria, eventos e incidentes, criterios de auditoria, lineamientos de seguridad de la información.

INTRODUCCIÓN

La información hoy en día es el activo más importante de una organización, por ende debe ser tratada con la importancia que corresponda según sea la valoración del activo y la necesidad de la misma. La seguridad de la información es la alternativa para salvaguardar los activos de información de cualquier organización, esta se basa en proteger los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad de los datos; para llevar a cabo esto s*e* cuenta con estándares y normas internacionales como las buenas prácticas contenidas en la Norma ISO/IEC 27002:2013 que dan cumplimientos a los controles establecidos de la Norma ISO/IEC 27001:2013.

Para la implantación e implementación de las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013 en una organización no es necesario que estas se encuentren certificadas, pueden servir como guía para una futura certificación, al decidir la alta dirección adquirir un compromiso con la seguridad de la información se deben definir políticas y lineamientos para el buen uso de la información y de los recursos tecnológicos. Para dar cumplimiento a estas políticas y lineamientos se hace necesario acudir a realizar auditorías de seguridad de la información y evidenciar así el cumplimiento de las mismas e identificar riesgos, amenazas y posibles vulnerabilidades.

La Universidad Autónoma de Occidente en pro de mejorar y generar un ambiente de seguridad de la información en sus instalaciones, ha venido trabajando y fortaleciendo el tema en su comunidad e infraestructura tecnológica; sin embargo al realizar una auditoría interna de seguridad de la información se obtienen resultados diferentes a lo esperado como consecuencia de la carencia de lineamientos, directrices y políticas para la ejecución de las mismas. Este proyecto identificará y propondrá mecanismos para la realización de auditorías internas de seguridad de la información, basándose en el Código de prácticas para la gestión de la seguridad de la información norma ISO/IEC 27002:2013, El sistema de gestión de seguridad de la información norma ISO/IEC 27001:2013, Directrices para la auditoría de sistemas de gestión de seguridad de la información norma ISO/IEC 27007:2011, Requisitos para los organismos que realizan la auditoría y certificación de sistemas de gestión de seguridad de la información norma ISO/IEC 27006:2011 y la norma ISO 19011:2011 directrices para la auditoría de sistemas de gestión.

Con el propósito de plantear a la Universidad Autónoma de Occidente la opción de aplicar auditorías internas de seguridad de la información, para la verificación de controles, políticas, buen uso de los recursos tecnológicos y de la información;

identificando así mejoras de seguridad de la información y posibles riesgos, abordando la toma de medidas preventivas y/o correctivas con controles normativos para la mitigación de los riesgos encontrados.

1. DESCRIPCIÓN DEL PROBLEMA

La Universidad Autónoma de Occidente ha adquirido un compromiso con la seguridad de la información en su comunidad e infraestructura tecnológica, en pro de mejorar y generar un ambiente de seguridad dentro y fuera de sus instalaciones. Sin embargo hoy en día al realizar una auditoría interna de seguridad de la información esta obtiene resultados diferentes a lo esperado, es decir se encuentran recomendaciones que no aplican por el modelo de negocio de la universidad; esto como consecuencia de la carencia de lineamientos, directrices y políticas para la ejecución de las mismas, por otro lado también se cuenta con diferentes administradores de plataforma tecnológica generando incertidumbre del cumplimiento del buen uso de los recursos tecnológicos, es por esto vital contar con mecanismos para la realización de auditorías internas de seguridad de la información sobre la comunidad y la infraestructura tecnológica de la Universidad.

2. ANTECEDENTES

El Ingeniero Jorge Armando Rojas Varela([*]) indico que antes de 2009 la coordinación de seguridad informática administraba plataforma tecnológica, dado que el perfil tenía unas actividades de administración de plataforma como respuesta de lineamientos de seguridad y todo lo que tuviera que ver con la seguridad informática. A partir de 2009 se da un cambio, se desliga todo el tema de plataforma, es decir, todo lo que es seguridad informática es responsabilidad del administrador o prestador del servicio (el que administra el servicio de correo debe saber seguridad para la plataforma de correo) desde ese momento queda claro quiénes son los responsables de seguridad de la plataforma tecnológica y de los servicios prestados.

La primera fase fue dejar claro quién es el responsable de seguridad sobre la infraestructura tecnológica, obteniendo así que para la plataforma sea cual sea su seguridad la debe garantizar el administrador de dicha plataforma.

¿Qué hace La coordinación de seguridad informática? La coordinación de seguridad informática brinda los lineamientos, políticas, estructuras, todo el gobierno de lo que es seguridad de la información. Cuando salen lineamientos de seguridad de la información de la coordinación, estos deben ser aplicados en los procesos de la universidad, sea con las personas y/o tecnología. Al hablar de tecnología cada uno es responsable de aplicar la seguridad, conduciendo así que al no haber lineamientos de seguridad para esa plataforma en particular el administrador debe responder por la seguridad y realizar actividades para garantizar que se está haciendo de la manera adecuada.

Actualmente se realizan auditorias, revisiones y acompañamiento, por la coordinación de seguridad informática o por el ente externo que es el revisor fiscal, sin embargo al adelantar estas actividades se desconoce el por qué se debe cumplir lo que se está diciendo, porque falta el marco regulatorio, el marco legal que indique que es responsabilidad hacer lo que se evidencia. Por ejemplo si se hace una revisión para verificar como se encuentran configurados el servicio web cuando pide toma de credenciales para la autenticación y falta un certificado digital que cifre la información, entonces en un documento se evidencia que se debería contar con un certificado digital que cifre la información de credenciales, porque pone en riesgo las credenciales de acceso y entonces afecta la seguridad de la información de la universidad; el documento se entrega, sin embargo no se

[*] ROJAS VARELA, Jorge Armando. Universidad Autónoma de Occidente. Cali, Colombia. Antecedentes, 2014.

implementa el certificado digital porque la falta recursos, tiempo, no es prioridad para la organización, etc. En últimas diferente a que sea la falta de recursos es la falta de concienciación y normalmente la concienciación la dan los lineamientos o políticas que vienen desde la alta dirección.

Por otro lado Los antecedentes de lo que se ha hecho en auditoria son actividades de revisoría fiscal por DELOITTE que hacen tres entradas al año:

Primera entrada, controles generales del sistema: se revisan controles de la computadora, políticas aplicadas, con cuales lineamientos se cuenta, cual es el marco de gobierno.

Segunda entrada transacciones significativas: revisan la parte contable, revisan como se garantiza desde el punto tecnológico que lo que sucede con respecto a las finanzas de la universidad se están manejando de manera adecuada, es decir que los componentes tecnológicos que soportan ese servicio están configurados de manera adecuada.

Tercera entrada, cierre contable de cada año: donde se revisa que se reporta en los sistemas y que se reporta contablemente.

La coordinación de seguridad informática interactúa aquí por el tema de los controles que tienen los componentes tecnológicos, para verificar si está configurado de manera adecuada o no. Como el revisor fiscal da recomendaciones, en algunos casos la universidad identifica que esas recomendaciones son para una entidad diferente a la universidad, por la cultura, por el modelo de negocio o por la forma en que se encuentran creados los procesos. Es decir, que las recomendaciones del revisor fiscal no son aplicadas en un ciento por ciento dado que algunas recomendaciones no aplican para el modelo de negocio de la universidad. Es aquí donde viene recomendaciones de 2010, 2011, 2012 que se encuentran en estado pendiente por que se identifica que no aplican, estas se identifican que son para otras entidades y se desconoce cómo funciona la Universidad Autónoma de Occidente por los revisores fiscales.

Con este proyecto se quiere llegar a la siguiente fase porque ya se están aprobando lineamientos con respecto a la aplicación de controles de seguridad, ya se está diciendo que se espera. Actualmente se encuentran aprobados la política de seguridad de la información, la política de privacidad de la información, la política de tratamiento de la información, política general de acceso a la

información, consultas, quejas y reclamos, para cubrir todo el tema de ley 1581, ya hay lineamientos que están cumpliendo, lineamientos que están siendo aplicados por la alta dirección.

Aprovechando los lineamientos que se encuentran aplicados y aprobados por la alta dirección, se desea contar con lineamientos y mecanismos oficiales de cómo adelantar una auditoria en seguridad de la información para que tenga un impacto mayor al que está teniendo hoy, e indicar que se debe hacer, como se debe hacer y verificar si se está cumpliendo.[*]

[*] ROJAS VARELA, Jorge Armando. Universidad Autónoma de Occidente. Cali, Colombia. Antecedentes, 2014.

3. JUSTIFICACIÓN

Las organizaciones necesitan demostrar en ocasiones que las labores que se realizan en su gestión son competentes y efectivas. En la seguridad de la información se debe demostrar la gestión del buen uso de los recursos tecnológicos y de la información, identificando y detectando los riesgos a los que se encuentran sometidos los activos de información, para abordar con los controles adecuados y mitigar los riesgos de la información.

La Coordinación de Seguridad Informática de la Universidad Autónoma de Occidente ha identificado que al realizarse hoy en día una revisión a los sistemas de gestión y a los procesos, se obtienen resultados diferentes a lo esperado, por la falta del marco regulatorio o políticas que indiquen como se debe realizar auditorías de seguridad de la información; teniendo en cuenta que la información tiene primordial importancia para el funcionamiento e incluso es determinante para la permanencia y supervivencia de la universidad, esta merece la revisión periódica que permita detallar e identificar el estado actual en que se encuentra los activos de información.

Las auditorias de seguridad de la información es la alternativa para verificar y dar diagnostico a la situación en que se encuentren los activos de información, generando como resultado información detallada a los responsables y custodios de los activos, que a su vez con esta información deberán buscar medidas preventivas y/o correctivas si es necesario, para evitar posibles eventos e incidentes de seguridad de la información.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Definir lineamientos tales como procedimientos, normas, políticas, estándares, líneas guía y líneas base para realizar auditorías de seguridad de la información siendo estas aplicadas sobre la infraestructura tecnológica de la Universidad Autónoma de Occidente.

4.2. OBJETIVOS ESPECÍFICOS

- Identificar el nivel de cumplimiento con respecto a las características y pilares de seguridad y privacidad de la información en la Institución

- Identificar y proponer mecanismos para el mejoramiento del procedimiento "Auditoria en Seguridad y Privacidad de la Información" de la Universidad.

- Identificar los requerimientos de seguridad y privacidad de la información estipulados en la norma ISO/IEC 27001:2013 y la norma ISO/IEC 27002:2013.

- Presentar recomendaciones sobre la implantación de medidas preventivas y correctivas al proceso de gestión de seguridad de la información.

- Brindar un diagnóstico a las medidas específicas de corrección.

- Validar por medio de prueba piloto los entregables del proyecto.

5. MARCO TEÓRICO

5.1 DEFINICIÓN DE SEGURIDAD DE LA INFORMACIÓN

La información es un activo que, como otros activos importantes del negocio, es esencial al negocio de una organización y requiere en consecuencia una protección adecuada. Esto es especialmente importante en ambientes de negocio cada vez más interconectados. Como consecuencia de esta creciente interconectividad, la información está ahora expuesta a un número mayor y a una variedad más amplia de amenazas y vulnerabilidades (véase también OECD - Guidelines for the Security of Information Systems and Networks). La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en filmes o hablada en conversación. Cualquiera sea la forma que tome la información o los medios por los que se comparta o almacene, la misma debería ser siempre protegida adecuadamente.

La seguridad de la información es la protección de la información contra una amplia gama de amenazas para asegurar la continuidad del negocio, minimizar los riesgos al negocio y maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizativas y funciones de hardware y software. Estos controles deberían ser establecidos, implementados, supervisados, revisados y mejorados cuando fuere necesario para asegurarse de que se cumplen los objetivos específicos de seguridad y de negocio de la organización. Esto debería hacerse en forma conjunta con otros procesos de la gestión del negocio.[1]

5.2 DEFINICIÓN DE SEGURIDAD INFORMÁTICA

“La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad

[1] INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Sistema de Gestión de Seguridad de la Información. NTC-ISO/IEC 27002. Bogotá D.C: ICONTEC, 2013. p. 54.

de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio."[2]

5.3 CARACTERÍSTICAS DE SEGURIDAD DE LA INFORMACIÓN

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. (ISO/IEC 13335-1: 2004).

Integridad: Propiedad de salvaguardar la exactitud y estado complete de los activos. (ISO/IEC 13335-1: 2004).

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. (ISO/IEC 13335-1: 2004).

Figura 1. Características de la seguridad de la información

Fuente: Blog de Seguridad INTECO, ¿Te preocupas por la seguridad de la información de tu empresa?, [en línea], consultado el 4 de Marzo del 2014, disponible en Internet: https://www.inteco.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/preocupas_seguridad_informacion_empresa

[2] Ibíd., p. 54.

5.4 FAMILIA ISO/IEC 27000:2014

Normas internacionales para los sistemas de gestión proporcionan un modelo a seguir en la creación y funcionamiento de un sistema de gestión. Este modelo incorpora los elementos sobre los que los expertos en la materia han llegado a un consenso como el estado internacional de la técnica. ISO/IECJTC1/SC 27 mantiene un comité de expertos dedicada a la elaboración de normas internacionales de sistemas de gestión de seguridad de la información, también conocido como el Sistema de Gestión de Seguridad de la Información (SGSI) de la familia de normas.[3]

5.4.1 SGSI familia de estándares

- ISO/IEC 27000 Sistemas de gestión de seguridad de la información - Información general y el vocabulario.

Alcance: Esta Norma Internacional proporciona a las organizaciones e individuos:

- una descripción general de la familia de normas de SGSI.
- una introducción a los sistemas de gestión de seguridad de la información (SGSI).
- los términos y definiciones que se utilizan en toda la familia de normas de SGSI.

Propósito: ISO / IEC 27000 describe los fundamentos de los sistemas de gestión de seguridad de información, que forman el sujeto de la familia de normas SGSI, y define términos relacionados.

- ISO/IEC 27001 Sistema de gestión de seguridad de la información – Requerimientos.

Alcance: Esta Norma Internacional especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el sistema de gestión

[3] NORMA INTERNACIONAL. Tecnología de la información – Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Información general y vocabulario. ISO/IEC 27000 3 ed. 2014. p. 31.

de seguridad de la información (SGSI) en el contexto de los riesgos globales de negocio de la organización. En él se especifica requisitos para la aplicación de los controles de seguridad de la información a medida de las necesidades de organizaciones individuales o partes de los mismos. Esta Norma Internacional puede ser utilizada por todas las organizaciones, independientemente del tipo, tamaño y naturaleza.

Propósito: ISO / IEC 27001 proporciona requisitos normativos para el desarrollo y operación de un SGSI, incluyendo un conjunto de controles para el control y mitigación de los riesgos asociados con el los activos de información que la organización pretende proteger mediante la operación de sus SGSI. Organizaciones funcionamiento de un SGSI puede tener su conformidad auditado y certificado. Los objetivos de control y controles del anexo A (ISO / IEC 27001) se seleccionarán como parte de este proceso del SGSI según corresponda para cubrir los requisitos identificados. Los objetivos de control y controles que se enumeran en la Tabla A.1 (ISO / IEC 27001) son directamente derivado de y alineado con los que figuran en la norma ISO / IEC 27002, las cláusulas 5 y 18.

- ISO/IEC 27002 Código de prácticas para los controles de seguridad de la información

Alcance: Esta Norma Internacional proporciona una lista de objetivos de control generalmente aceptados, y las mejores prácticas de control para ser utilizado como una guía de implementación en la selección y la aplicación de controles para lograr la seguridad de la información.

Propósito: ISO / IEC 27002 proporciona orientación sobre la aplicación de los controles de seguridad de la información.

En concreto las cláusulas 5 y 18 proporcionan asesoramiento sobre la ejecución específica y orientación sobre las mejores prácticas en apoyo de los controles especificados en las cláusulas A.5 al A.18 de la norma ISO / IEC 27001.

- ISO/IEC 27003 Orientación para la implementación del sistema de gestión de seguridad de la información

Alcance: Esta Norma Internacional proporciona orientación para la implementación práctica y proporciona, además, información para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI según ISO/IEC 27001.

Propósito: ISO/IEC 27003 proporciona un enfoque orientado a procesos para la implementación exitosa del SGSI según ISO/IEC 27001.

- ISO/IEC 27004 Gestión de la seguridad de la información – Medición

Alcance: Esta Norma Internacional proporciona orientación y asesoramiento sobre el desarrollo y uso de mediciones con el fin de evaluar la eficacia del SGSI, objetivos de control y controles utilizados para implementar y administrar la seguridad de la información, tal como se especifica en la norma ISO/IEC 27001.

Propósito: ISO/IEC 27004 proporciona un marco de medición que permite una evaluación del SGSI eficacia que se mide de acuerdo con ISO/IEC 27001.[4]

- ISO/IEC 27005 Gestión del riesgo de seguridad de la información

Alcance: Esta norma proporciona las directrices para la gestión de riesgos de seguridad de la información. El método descrito en esta Norma Internacional apoya los conceptos generales especificados en ISO/IEC 27001.

Propósito: ISO/IEC 27005 proporciona orientación sobre la aplicación de una gestión de riesgos orientado a los procesos acercarse para ayudar en forma satisfactoria la implementación y el cumplimiento de la gestión del riesgo de la seguridad de la información requisitos de la norma ISO/IEC 27001.

- ISO/IEC 27006 Requisitos para los organismos que realizan la auditoría y la certificación de seguridad de la información sistemas de gestión

Alcance: Esta norma internacional especifica los requisitos y proporciona una guía para los organismos que realizan auditoría y certificación del SGSI según

[4] Ibíd., p. 31.

ISO/IEC 27001, además de los requisitos contenida en la norma ISO/IEC 17021. Está pensado principalmente para apoyar la acreditación de la certificación organismos que realizan la certificación de SGSI según ISO/IEC 27001.

Propósito: ISO/IEC 27006 suplementos ISO/IEC 17021 en la prestación de los requisitos por los cuales organizaciones de certificación están acreditados, lo que permite a estas organizaciones para proporcionar el cumplimiento certificaciones consistentemente contra los requisitos establecidos en la norma ISO/IEC 27001.

- ISO/IEC 27007 Directrices para la auditoría de sistemas de gestión de seguridad de la información

Alcance: Esta Norma Internacional proporciona orientación sobre la realización de auditorías del SGSI, así como orientación en la competencia de los auditores de sistemas de gestión de la seguridad de la información, además de la orientación contenida en la norma ISO 19011, que es aplicable a los sistemas de gestión en general.

Propósito: ISO/IEC 27007 proporcionará orientación a las organizaciones que necesitan para llevar a cabo interna o auditorías externas de un SGSI o para administrar un programa de auditoría SGSI según los requisitos especificados en la norma ISO/IEC 27001.[5]

- ISO/IEC TR 27008 Directrices para los auditores sobre los controles de seguridad de la información

Alcance: El presente informe técnico proporciona orientación sobre la revisión de la implementación y operación de controles, incluyendo la comprobación del cumplimiento técnico de los controles del sistema de información, de conformidad con establecidos estándares de seguridad de la información de una organización.

Propósito: El presente informe técnico proporciona un enfoque en la revisión de los controles de seguridad de la información, incluidos la comprobación de la conformidad técnica, frente a un estándar de implementación de seguridad de la información, que establecido por la organización. No tiene la intención de proporcionar una orientación específica sobre el cumplimiento comprobación en relación con la medición, la evaluación de riesgos o auditoría de un SGSI según lo especificado en la norma ISO/IEC 27004, ISO/IEC 27005 o ISO/IEC 27007,

[5] Ibíd., p. 31.

respectivamente. Este Informe Técnico no está diseñado para la gestión de auditorías de sistemas.

- ISO/IEC 27010 Gestión de seguridad de la información para inter-sectorial e inter-organizacional comunicaciones

Alcance: Esta Norma Internacional proporciona directrices, además de la orientación que figuran en el ISO/IEC 27000 de la familia de normas para la aplicación de gestión de seguridad de la información dentro de las comunidades y, además, la información proporciona controles y orientaciones relacionadas específicamente para iniciar, implementar, mantener y mejorar la seguridad de la información en la inter-organizacional y las comunicaciones inter-sectoriales.

Propósito: Esta Norma Internacional es aplicable a todas las formas de intercambio y difusión de información sensible, tanto pública como privada, a nivel nacional e internacional, dentro del mismo sector o mercado sector o entre sectores. En particular, puede ser aplicable a los intercambios de información y e intercambio relacionados con el suministro, el mantenimiento y la protección de los del estado de la nación de la organización o crítica infraestructura.

- ISO/IEC 27011 Directrices de gestión de la seguridad de la información para las organizaciones de telecomunicaciones basado en la norma ISO/IEC 27002[6]

Alcance: Esta norma proporciona directrices que fomenten la aplicación de la información Gestión de la seguridad en las organizaciones de telecomunicaciones.

Propósito: ISO/IEC 27011 proporciona a las organizaciones de telecomunicaciones con una adaptación de la ISO/IEC 27002 directrices únicas para su sector industrial que sean adicionales a las orientaciones proporcionadas hacia el cumplimiento de los requisitos de la norma ISO/IEC 27001, en el anexo A.

- ISO/IEC 27013 Orientación sobre la aplicación integrada de ISO/IEC 27001 e ISO/IEC 20000-1

[6] Ibíd., p. 31.

Alcance: Esta Norma Internacional proporcionará orientación sobre la aplicación integrada de ISO/IEC 27001 e ISO/IEC 20000-1 para las organizaciones con la intención de:

"a) implementar la norma ISO/IEC 27001 para el ISO/IEC 20000-1 ya está aprobada, o viceversa;
b) aplicar las normas ISO/IEC 27001 e ISO/IEC 20000-1 juntos;
c) alinear la Norma ISO/IEC 27001 e ISO/IEC 20000-1 implementaciones de sistemas de gestión existentes."[7]

Propósito: proporcionar a las organizaciones una mejor comprensión de las características, semejanzas y diferencias de la norma ISO/IEC 27001 e ISO/IEC 20000-1 para ayudar en la planificación de una gestión integrada sistema que se ajusta tanto a las Normas Internacionales.

- ISO/IEC 27014 Gobernanza de la seguridad informática

Alcance: Esta Norma Internacional proporcionará orientación sobre los principios y procesos para la gobernabilidad de seguridad de la información, mediante el cual las organizaciones pueden evaluar, dirigir y supervisar la gestión de la seguridad de la información.

Propósito: Seguridad de la información se ha convertido en una cuestión clave para las organizaciones. No sólo hay cada vez mayor requisitos normativos, sino también el fracaso de las medidas de seguridad de la información de una organización puede tener un impacto directo en la reputación de una organización. Por lo tanto, los órganos de gobierno, como parte de su responsabilidades de gobierno, se les exige cada vez más a tener la supervisión de seguridad de la información garantizar los objetivos de la organización son alcanzados.[8]

- ISO/IEC TR 27015 Directrices de gestión de seguridad de la información para los servicios financieros

Alcance: Este Informe Técnico proporciona directrices, además de la orientación dada en la norma ISO/IEC 27000 familia de normas, para iniciar, implementar,

[7] Ibíd., p. 31
[8] Ibíd., p. 31.

mantener y mejorar la seguridad de la información dentro de las organizaciones que prestan servicios financieros.

Propósito: El presente informe técnico es un suplemento especializado para ISO/IEC 27001 e ISO/IEC 27002 Normas internacionales para el uso de organizaciones que ofrecen servicios financieros para apoyarlos en:

"a) iniciar, implementar, mantener y mejorar un sistema de gestión de seguridad de la información basado en la norma internacional ISO/IEC 27001
b) Diseñar e implementar controles definidos en la Norma Internacional o ISO/IEC 27002 dentro de esta Norma Internacional."[9]

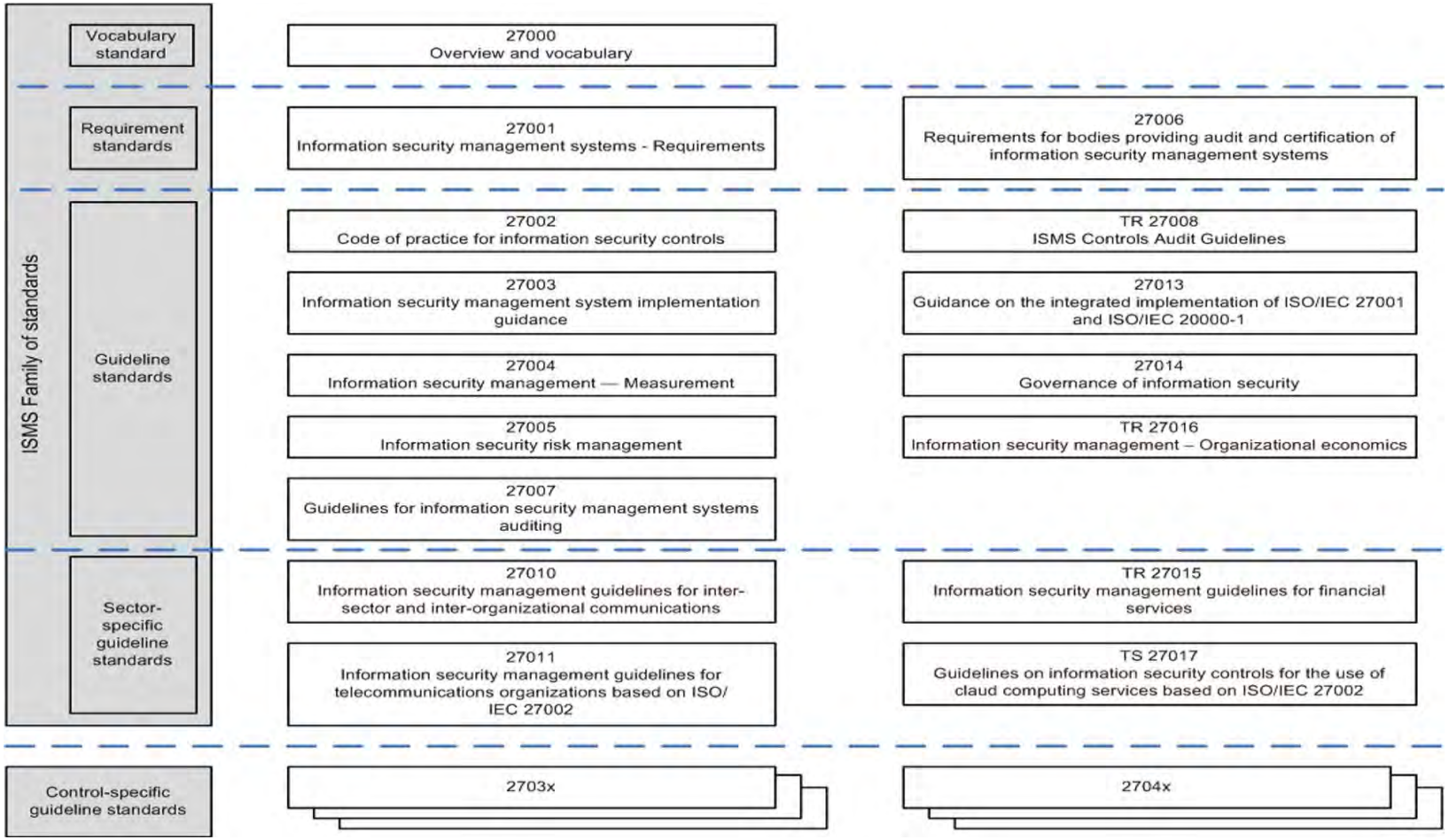
- ISO/IEC TR 27016 Gestión de la seguridad de la información - Economía de las Organizaciones

Alcance: El presente informe técnico proporcionará una metodología que permita a las organizaciones a comprender mejor económicamente cómo valorar con mayor precisión sus activos de información identificadas, el valor del potencial riesgos para los activos de información, aprecian el valor que los controles de protección de la información ofrecen a estos activos de información, y determinar el nivel óptimo de los recursos que deben aplicarse en la obtención de estos los activos de información.

Propósito: El presente Informe Técnico complementará la familia de normas de SGSI superponiendo una perspectiva de la economía en la protección de los activos de información de una organización en el contexto de la entorno social más amplio en el que opera una organización y proporcionar orientación sobre cómo aplicar economía de las organizaciones de seguridad de la información mediante el uso de modelos y ejemplos.

[9] Ibíd., p. 31.

Figura 2. SGSI Familia 27000



Fuente: SGSI familia de normas, información general. Norma internacional. Tecnología de la información – Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Información general y vocabulario. ISO/IEC 27000 3 ed. 2014. 31p.

5.4.2 Norma ISO/IEC 27001:2013. Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la segundad de la información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos aspectos y sus sistemas de apoyo cambien con el tiempo. Se espera que la implementación de un SGSI se ajuste de acuerdo con las necesidades de la organización, por ejemplo, una situación simple requiere una solución de SGSI simple.

Esta norma se puede usar para evaluar la conformidad, por las partes interesadas, tanto internas como externas.[10]

La estructura de la norma ISO / IEC 27001:2013 es de la siguiente manera:

- 0 Introducción
- 1 Ámbito de aplicación
- 2 Referencias normativas
- 3 Términos y definiciones
- 4 Contexto de la organización
- 5 Liderazgo
- 6 Planificación
- 7 Apoyo
- 8 Funcionamiento
- 9 La evaluación del desempeño
- 10 Mejoramiento

Norma que especifica los requisitos para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar un SGSI documentado dentro del contexto global de los riesgos de negocio de la organización. Especifica los requisitos para la implantación de los controles de seguridad hechos a medida de las necesidades de las organizaciones individuales o partes de la misma.

Se adopta el modelo PHVA (planear, hacer, verificar y actuar) para todos los procesos de la organización.[11]

[10] INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Sistema de Gestión de Seguridad de la Información. NTC-ISO/IEC 27001. Bogotá D.C: ICONTEC, 2013. 54p.

5.4.2.1 ¿Que es un sistema de gestión de seguridad de la información SGSI)? Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar. Hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.[12]

5.4.2.2 Diferencias anexo a (normativo) ISO/IEC 27001 de 2005 al 2013. Anexo 2005. Los objetivos de control y los controles enumerados en la Tabla A.I se han obtenido exactamente de los de la NTC-ISO/IEC 17799:2005, numerales 5 a 15, y están alineados con ellos. Las listas de estas tablas no son exhaustivas, y la organización puede considerar que se necesitan objetivos de control y controles adicionales. Los objetivos de control y controles de estas tablas se deben seleccionar como parte del proceso de SCSI especificado en el numeral 4.2.1.

La norma NTC- ISO/IEC 17799:2005, numerales 5 a 15, proporciona asesoría y orientación sobre las mejores prácticas de apoyo a los controles especificados en el literal A.5 a A.15.[13]

Anexo 2013. El número de controles se ha reducido de 133 a 114, mientras que el número de secciones ha aumentado desde 11 a 14. Los cambios han sido un resultado de la eliminación de algunos controles, la combinación de los demás y la introducción de algunos nuevos.[14]

Los puntos del Anexo A son ahora de la siguiente manera:

- 5. Políticas de seguridad Información
- 6. Organización de la seguridad de la información
- 7. la seguridad de los recursos humanos
- 8. Gestión de activos
- 9. control de acceso
- 10. Criptografía
- 11. La seguridad física y ambiental

---

[11] ISO/IEC 2700[en línea]. Peru: Tecnologias y Negocios en Telecomunicaciones en el Perú y Latinoamérica, Felipe Reyes Vivanco 2013, [consultado 15 de Diciembre de 2013]. Disponible en Internet: http://www.felipereyesvivanco.com/direccion-de-proyectos/isoiec-27000/

[12] Op. Cit p. 54.

[13] Op. Cit p. 54.

[14] NUEVA ISO / IEC 27001:2013, Controles cruzados referencia el Anexo A de la norma ISO/IEC 27001:2013 de ISO/IEC 27001:2005, [en línea], consultado el 4 de Marzo del 2014, file:///C:/Users/gprendon/Downloads/New%20ISO-IEC%2027001%20transition%20guide.pdf

- 12. Seguridad de Operaciones
- 13. Seguridad de Comunicaciones
- 14. Sistema de adquisición, desarrollo y mantenimiento
- 15. Las relaciones con proveedores
- 16.Información de gestión de incidentes de seguridad
- 17. Aspectos de seguridad de información de gestión de la continuidad del negocio
- 18. Cumplimiento

Tabla 1. Controles cruzados referencia el Anexo A de la norma ISO/IEC 27001:2013 de ISO/IEC 27001:2005

	ISO/IEC 27001 2005										
ISO/IEC 27001:2013	A.5	A.6	A.7	A.8	A.9	A.10	A.11	A.12	A.13	A.14	A.15
A.5 Política de Seguridad de la información											
A.5.1 Dirección de Gestión de seguridad de la información	x										
6. Organización de la seguridad de la información											
A.6.1 organización interna		x		x		x					
A.6.2 dispositivos móviles y el teletrabajo							x				
7. la seguridad de los recursos humanos											
A.7.1 Antes de empleo				x							
A.7.2 Durante el empleo				x							
A.7.3 Terminación y cambio de empleo				x							
8. Gestión de activos											
A.8.1 Responsabilidad de los activos			x	x							
A.8.2 Clasificación de la información						x					

Tabla 1. (Continuación)

A.8.2 Clasificación de la información						x					
A.8.3 Manejo de Medios						x					
9. control de acceso											
A.9.1 Requisitos de negocio para el control de acceso							x				
A.9.2 Gestión de acceso al usuario							x				
A.9.3 Responsabilidades de usuario							x				
A.9.4 Control del sistema y aplicación de acceso							x	x			
10. Criptografía											
A.10.1 Controles criptográficos								x			
11. La seguridad física y ambiental											
A.11.1 Las áreas seguras						x					
A.11.2 Equipo						x					
12. Seguridad de Operaciones											
A.12.1 Procedimientos y responsabilidades operacionales							x				
A.12.2 Protección del malware							x				
A.12.3 de copia de seguridad							x				
A.12.4 Logging y monitoreo							x				
A.12.5 Control de del software operativo									x		
A.12.6 Gestión de vulnerabilidades Técnica									x		
A.12.7 Consideraciones de auditoría de sistemas de información											x
13. Seguridad de Comunicaciones											
A.13.1 Gestión de la seguridad en la Red						x	x				
A.13.2 La transferencia de información						x					

Tabla 1. (Continuación)

14. Sistema de adquisición, desarrollo y mantenimiento											
A.14.1 Requisitos de seguridad para sistemas de información						x		x			
A.14.2 Seguridad en los procesos de desarrollo y soporte						x		x			
A.14.3 Los datos de prueba								x			
15. Las relaciones con proveedores											
A.15.1 Seguridad de la información en relaciones con los proveedores		x									
A.15.2 Gestión de la prestación de servicios Proveedor						x					
16. Información de gestión de incidentes de seguridad											
A.16.1 Gestión de incidentes y gestión de seguridad de la información									x		
17. Aspectos de seguridad de información de gestión de la continuidad del negocio											
A.17.1 Información continuidad seguridad										x	
A.17.2 despidos											
18. Cumplimiento											
A.18.1 El cumplimiento de los requisitos legales											x
A.18.2 Información revisiones de seguridad										x	

Fuente: NUEVA ISO / IEC 27001:2013, Controles cruzados referencia el Anexo A de la norma ISO/IEC 27001:2013 de ISO/IEC 27001:2005, [en línea], consultado el 4 de Marzo del 2014, file:///C:/Users/gprendon/Downloads/New%20ISO-IEC%2027001%20transition%20guide.pdf

5.4.3 Norma ISO/IEC 27002. Esta Norma Internacional establece guías y principios generales para iniciar, implantar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos señalados en esta

norma internacional proporcionan orientaciones generales sobre las metas comúnmente aceptadas para la gestión de la seguridad de la información.

Los objetivos de control y los controles de esta norma internacional están pensados para ser implementados a fin de alcanzar los requisitos identificados por una evaluación del riesgo. Esta norma internacional puede servir como guía práctica para desarrollar normas de seguridad de la organización y una práctica eficaz de la gestión de la misma, así como ayudar a construir confianza en las actividades entre organizaciones.[15]

La norma ISO 27002 fue publicada originalmente como un cambio de nombre de la norma ISO 17799, la cual se basaba en un documento publicado por el gobierno del Reino Unido, que se convirtió en estándar en 1995. Fue en el 2000 cuando se publicó por primera vez como ISO 17799, y en 2005 aparece una nueva versión, junto con la publicación de la norma ISO 27001. No debe olvidarse que estos dos documentos están destinados a ser utilizados de forma complementaria.

Dentro de ISO/IEC 27002 se extiende la información de los renovados anexos de ISO/IEC 27001-2013, donde básicamente se describen los dominios de control y los mecanismos de control, que pueden ser implementados dentro de una organización, siguiendo las directrices de ISO 27001. En esta nueva versión de la norma se encuentran los controles que buscan mitigar el impacto o la posibilidad de ocurrencia de los diferentes riesgos a los cuales se encuentra expuesta la organización.

Dentro de los cambios interesantes de resaltar que lo relacionado con dispositivos móviles y teletrabajo que antes estaba asociado al Control de Accesos, ahora se encuentra dentro de la sección 6 “Organización de la Seguridad de la Información”. Y dentro de la sección de Control de Accesos se engloba lo relacionado con acceso al sistema operativo, a las aplicaciones y la información. Todo lo relacionado con Criptografía es un dominio de control nuevo, sección 10, dentro de la cual se incluyen todo los controles criptográficos sugeridos para una organización. En el caso de los controles que deben tenerse en cuenta en el caso de la recuperación de desastres están dentro de la sección 17.

Además cabe resaltar que existen versiones específicas de la norma ISO/IEC 27002, enfocadas en diferentes tipos de empresas: manufactureras, sector de la salud, sector financiero, entre otros. Si bien la nomenclatura ISO es diferente, son

[15] Ibíd., p. 133.

normas que toman como referencia la ya mencionada ISO 27002 y por tanto lo tanto están alienados para la correcta gestión de la seguridad de la información.[16]

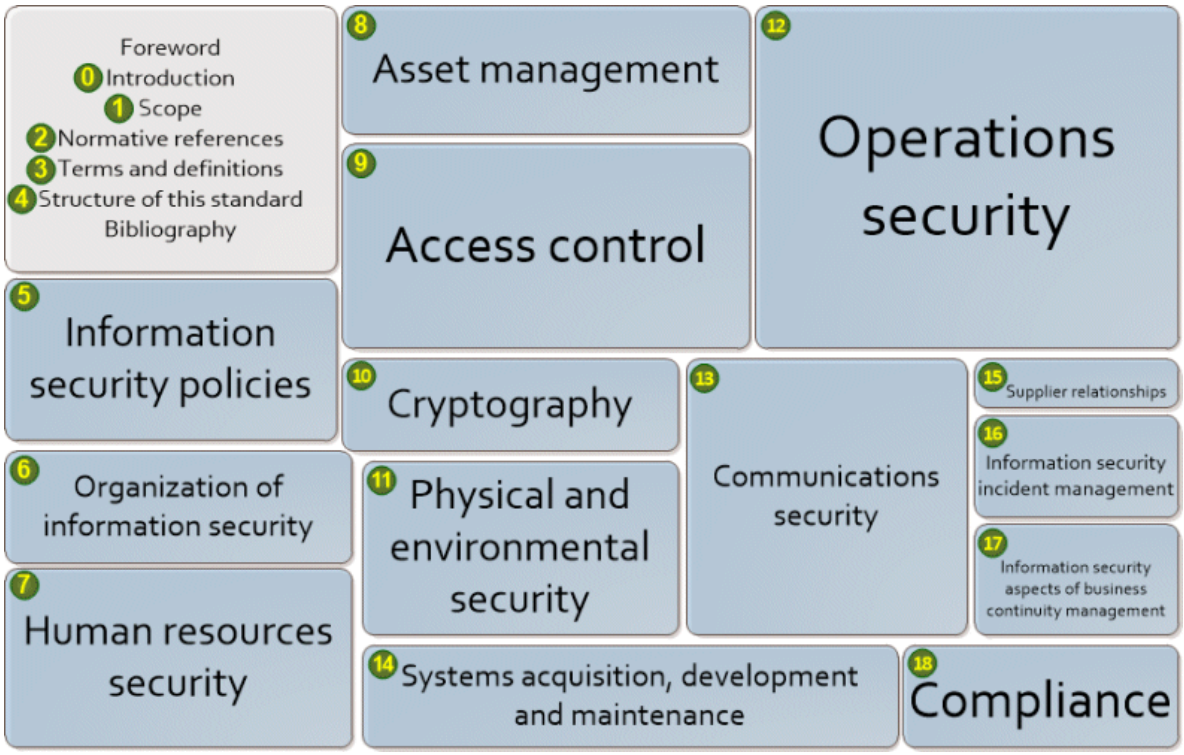
27002:2005 Esta norma contiene 11 capítulos de control de la seguridad que en su conjunto contienen un total de 39 categorías principales de seguridad y un capítulo introductorio a la evaluación y tratamiento de riesgos. [17]

Figura 3. Estructura de los dominios de la Norma ISO/IEC 27001:2005

Fuente: Normas, estándares, Leyes y demás de las políticas de seguridad, ISO 27002, [en línea], consultado el 4 de Marzo del 2014, disponible en Internet: http://seguridadinformaticaufps.wikispaces.com/Normas,+estandares,+Leyes+y+demas+de+las+politicas+de+seguridad.+1150204-159-250-214

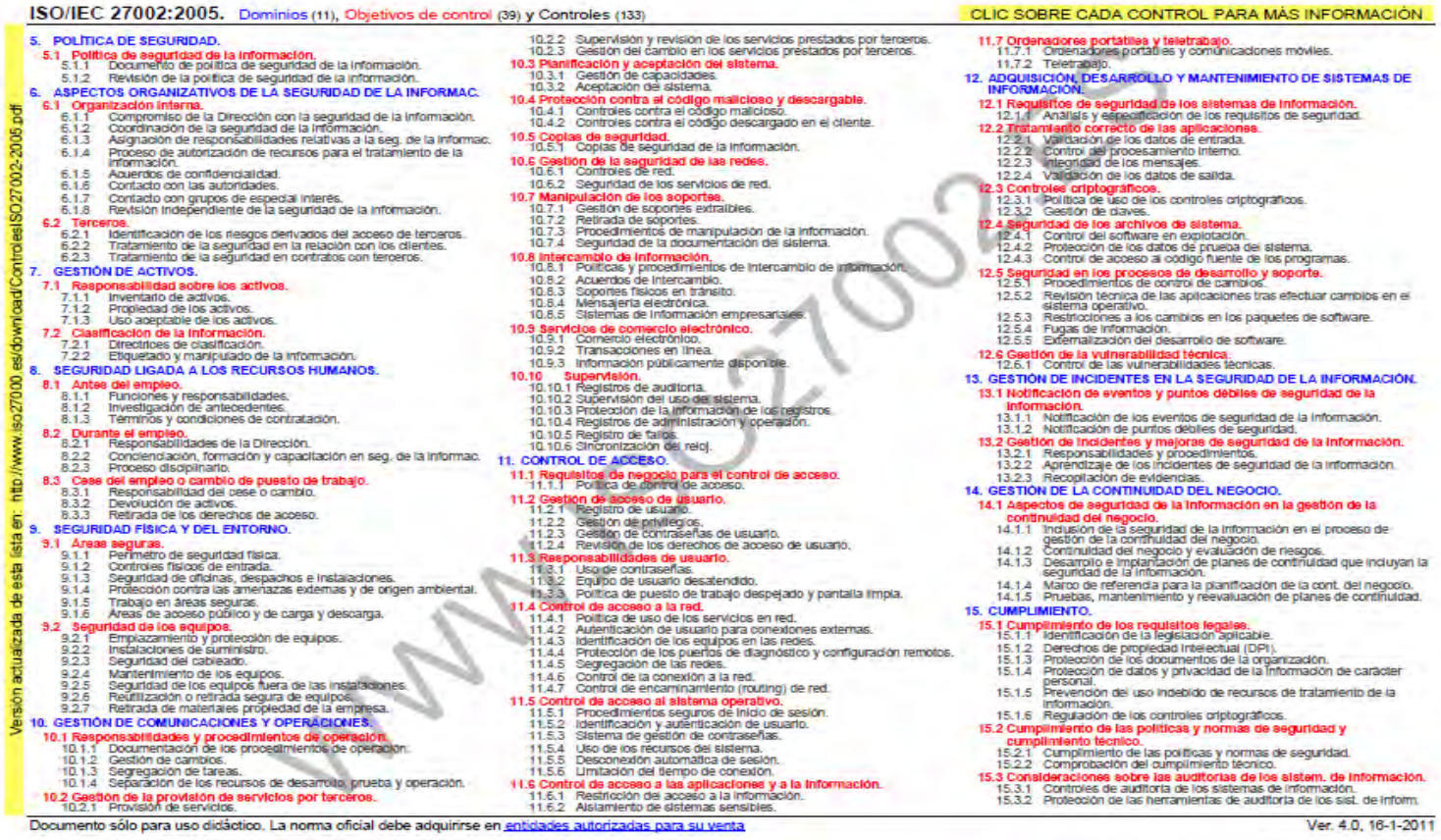
[16] GUTIERREZ AMAYA, Camilo, Welivesecurity, ISO/IEC 27002:2013 y los cambios en los dominios de control, [en línea], consultado el 04 de marzo del 2014, disponible en Internet: http://www.welivesecurity.com/la-es/2013/12/12/iso-iec-27002-2013-cambios-dominios-control/
[17] Ibíd., p. 133.

Figura 4. Estructura de los dominios de la Norma ISO/IEC 27002:2013



Fuente: ISO/IEC 27002, SO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls, [en línea], consultado el 4 de Marzo del 2014, disponible en Internet: http://www.iso27001security.com/html/27002.html

Figura 5. Controles Norma ISO/IEC 27002: 2005



ISO/IEC 27002:2005. Dominios (11), Objetivos de control (39) y Controles (133)

CLIC SOBRE CADA CONTROL PARA MÁS INFORMACIÓN

Versión actualizada de esta lista en: http://www.iso27000.es/download/ControlesISO27002-2005.pdf

5. POLITICA DE SEGURIDAD.
5.1 Política de seguridad de la información.
5.1.1 Documento de política de seguridad de la información.
5.1.2 Revisión de la política de seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Compromiso de la Dirección con la seguridad de la información.
6.1.2 Coordinación de la seguridad de la información.
6.1.3 Asignación de responsabilidades relativas a la seg. de la informac.
6.1.4 Proceso de autorización de recursos para el tratamiento de la información.
6.1.5 Acuerdos de confidencialidad.
6.1.6 Contacto con las autoridades.
6.1.7 Contacto con grupos de especial interés.
6.1.8 Revisión independiente de la seguridad de la información.
6.2 Terceros.
6.2.1 Identificación de los riesgos derivados del acceso de terceros.
6.2.2 Tratamiento de la seguridad en la relación con los clientes.
6.2.3 Tratamiento de la seguridad en contratos con terceros.
7. GESTIÓN DE ACTIVOS.
7.1 Responsabilidad sobre los activos.
7.1.1 Inventario de activos.
7.1.2 Propiedad de los activos.
7.1.3 Uso aceptable de los activos.
7.2 Clasificación de la información.
7.2.1 Directrices de clasificación.
7.2.2 Etiquetado y manipulado de la información.
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
8.1 Antes del empleo.
8.1.1 Funciones y responsabilidades.
8.1.2 Investigación de antecedentes.
8.1.3 Términos y condiciones de contratación.
8.2 Durante el empleo.
8.2.1 Responsabilidades de la Dirección.
8.2.2 Concienciación, formación y capacitación en seg. de la informac.
8.2.3 Proceso disciplinario.
8.3 Cese del empleo o cambio de puesto de trabajo.
8.3.1 Responsabilidad del cese o cambio.
8.3.2 Devolución de activos.
8.3.3 Retirada de los derechos de acceso.
9. SEGURIDAD FÍSICA Y DEL ENTORNO.
9.1 Áreas seguras.
9.1.1 Perímetro de seguridad física.
9.1.2 Controles físicos de entrada.
9.1.3 Seguridad de oficinas, despachos e instalaciones.
9.1.4 Protección contra las amenazas externas y de origen ambiental.
9.1.5 Trabajo en áreas seguras.
9.1.6 Áreas de acceso público y de carga y descarga.
9.2 Seguridad de los equipos.
9.2.1 Emplazamiento y protección de equipos.
9.2.2 Instalaciones de suministro.
9.2.3 Seguridad del cableado.
9.2.4 Mantenimiento de los equipos.
9.2.5 Seguridad de los equipos fuera de las instalaciones.
9.2.6 Reutilización o retirada segura de equipos.
9.2.7 Retirada de materiales propiedad de la empresa.
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.
10.1 Responsabilidades y procedimientos de operación.
10.1.1 Documentación de los procedimientos de operación.
10.1.2 Gestión de cambios.
10.1.3 Segregación de tareas.
10.1.4 Separación de los recursos de desarrollo, prueba y operación.
10.2 Gestión de la provisión de servicios por terceros.
10.2.1 Provisión de servicios.
10.2.2 Supervisión y revisión de los servicios prestados por terceros.
10.2.3 Gestión del cambio en los servicios prestados por terceros.
10.3 Planificación y aceptación del sistema.
10.3.1 Gestión de capacidades.
10.3.2 Aceptación del sistema.
10.4 Protección contra el código malicioso y descargable.
10.4.1 Controles contra el código malicioso.
10.4.2 Controles contra el código descargado en el cliente.
10.5 Copias de seguridad.
10.5.1 Copias de seguridad de la información.
10.6 Gestión de la seguridad de las redes.
10.6.1 Controles de red.
10.6.2 Seguridad de los servicios de red.
10.7 Manipulación de los soportes.
10.7.1 Gestión de soportes extraíbles.
10.7.2 Retirada de soportes.
10.7.3 Procedimientos de manipulación de la información.
10.7.4 Seguridad de la documentación del sistema.
10.8 Intercambio de información.
10.8.1 Políticas y procedimientos de intercambio de información.
10.8.2 Acuerdos de intercambio.
10.8.3 Soportes físicos en tránsito.
10.8.4 Mensajería electrónica.
10.8.5 Sistemas de información empresariales.
10.9 Servicios de comercio electrónico.
10.9.1 Comercio electrónico.
10.9.2 Transacciones en línea.
10.9.3 Información públicamente disponible.
10.10 Supervisión.
10.10.1 Registros de auditoría.
10.10.2 Supervisión del uso del sistema.
10.10.3 Protección de la información de los registros.
10.10.4 Registros de administración y operación.
10.10.5 Registro de fallos.
10.10.6 Sincronización del reloj.
11. CONTROL DE ACCESO.
11.1 Requisitos de negocio para el control de acceso.
11.1.1 Política de control de acceso.
11.2 Gestión de acceso de usuario.
11.2.1 Registro de usuario.
11.2.2 Gestión de privilegios.
11.2.3 Gestión de contraseñas de usuario.
11.2.4 Revisión de los derechos de acceso de usuario.
11.3 Responsabilidades de usuario.
11.3.1 Uso de contraseñas.
11.3.2 Equipo de usuario desatendido.
11.3.3 Política de puesto de trabajo despejado y pantalla limpia.
11.4 Control de acceso a la red.
11.4.1 Política de uso de los servicios en red.
11.4.2 Autenticación de usuario para conexiones externas.
11.4.3 Identificación de los equipos en las redes.
11.4.4 Protección de los puertos de diagnóstico y configuración remotos.
11.4.5 Segregación de las redes.
11.4.6 Control de la conexión a la red.
11.4.7 Control de encaminamiento (routing) de red.
11.5 Control de acceso al sistema operativo.
11.5.1 Procedimientos seguros de inicio de sesión.
11.5.2 Identificación y autenticación de usuario.
11.5.3 Sistema de gestión de contraseñas.
11.5.4 Uso de los recursos del sistema.
11.5.5 Desconexión automática de sesión.
11.5.6 Limitación del tiempo de conexión.
11.6 Control de acceso a las aplicaciones y a la información.
11.6.1 Restricción del acceso a la información.
11.6.2 Aislamiento de sistemas sensibles.
11.7 Ordenadores portátiles y teletrabajo.
11.7.1 Ordenadores portátiles y comunicaciones móviles.
11.7.2 Teletrabajo.
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.
12.1 Requisitos de seguridad de los sistemas de información.
12.1.1 Análisis y especificación de los requisitos de seguridad.
12.2 Tratamiento correcto de las aplicaciones.
12.2.1 Validación de los datos de entrada.
12.2.2 Control del procesamiento interno.
12.2.3 Integridad de los mensajes.
12.2.4 Validación de los datos de salida.
12.3 Controles criptográficos.
12.3.1 Política de uso de los controles criptográficos.
12.3.2 Gestión de claves.
12.4 Seguridad de los archivos de sistema.
12.4.1 Control del software en explotación.
12.4.2 Protección de los datos de prueba del sistema.
12.4.3 Control de acceso al código fuente de los programas.
12.5 Seguridad en los procesos de desarrollo y soporte.
12.5.1 Procedimientos de control de cambios.
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
12.5.3 Restricciones a los cambios en los paquetes de software.
12.5.4 Fugas de información.
12.5.5 Externalización del desarrollo de software.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Control de las vulnerabilidades técnicas.
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
13.1 Notificación de eventos y puntos débiles de seguridad de la información.
13.1.1 Notificación de los eventos de seguridad de la información.
13.1.2 Notificación de puntos débiles de seguridad.
13.2 Gestión de incidentes y mejoras de seguridad de la información.
13.2.1 Responsabilidades y procedimientos.
13.2.2 Aprendizaje de los incidentes de seguridad de la información.
13.2.3 Recopilación de evidencias.
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
14.1.2 Continuidad del negocio y evaluación de riesgos.
14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
14.1.4 Marco de referencia para la planificación de la cont. del negocio.
14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.
15. CUMPLIMIENTO.
15.1 Cumplimiento de los requisitos legales.
15.1.1 Identificación de la legislación aplicable.
15.1.2 Derechos de propiedad intelectual (DPI).
15.1.3 Protección de los documentos de la organización.
15.1.4 Protección de datos y privacidad de la información de carácter personal.
15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.
15.1.6 Regulación de los controles criptográficos.
15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.
15.2.1 Cumplimiento de las políticas y normas de seguridad.
15.2.2 Comprobación del cumplimiento técnico.
15.3 Consideraciones sobre las auditorías de los sistem. de información.
15.3.1 Controles de auditoría de los sistemas de información.
15.3.2 Protección de las herramientas de auditoría de los sist. de inform.

Documento sólo para uso didáctico. La norma oficial debe adquirirse en entidades autorizadas para su venta

Ver. 4.0, 16-1-2011

Fuente: ISO/IEC 27002:2005, Dominios (11), Objetivos de control (39) y controles (133), *[en línea], consultado el 5 de Marzo del 2014,* disponible en Internet: http://www.iso27000.es/download/ControlesISO27002-2005.pdf*

* **Observación, se tendrá en cuenta todavía la norma ISO/IEC 27001:2005 y la norma ISO/IEC 27002:2005, debido a que la organización aun trabaja con estas normas, cabe aclarar que se propondrán las respectivas mejoras para migrar a la norma actualizada de 2013**

5.4.4 Norma ISO 19011:2011. Esta Norma Internacional no establece requisitos, sino que provee una guía sobre el manejo de un programa de auditoría, sobre la planeación y realización de una auditoría a un sistema de gestión, así como sobre la competencia y evaluación de un auditor que pertenezca al equipo auditor. Las organizaciones pueden tener y operar más de un sistema de gestión formal. Para simplificar la lectura de esta Norma Internacional, se preferirá la forma singular de —Sistema de Gestión‖, pero el lector puede adaptar la implementación de la guía a su propia situación particular. Esto también aplica para el uso de —persona y —personas, —auditor y —auditores. [18]

5.4.4.1 Auditoria. Proceso sistemático, independiente y documentado para obtener evidencias de la auditoría (3.3) y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de auditoría (3.2).

Nota 1 Las auditorías internas, denominadas en algunos casos como auditorías de primera parte, se realizan por, o en nombre de, la propia organización, para la revisión por la dirección y con otros fines internos (ej. para confirmar la efectividad del sistema de gestión o para obtener información para la mejora del sistema de gestión). Las auditorías internas pueden constituir la base para la autodelcaración de conformidad de una organización. En muchos casos, particularmente en organizaciones pequeñas, la independencia puede demostrarse al estar el auditor libre de responsabilidad de la actividad que se audita o libre de prejuicios o conflicto de intereses.

Nota 2 Las auditorías externas incluyen lo que se denomina generalmente auditorías de segunda y tercera parte. Las auditorías de segunda parte se llevan a cabo por partes que tienen un interés en la organización, tal como los clientes, o por otras personas en su nombre. Las auditorías de tercera parte se llevan a cabo por organizaciones auditoras independientes y externas, tales como aquellas que proporcionan el registro o la certificación de conformidad.

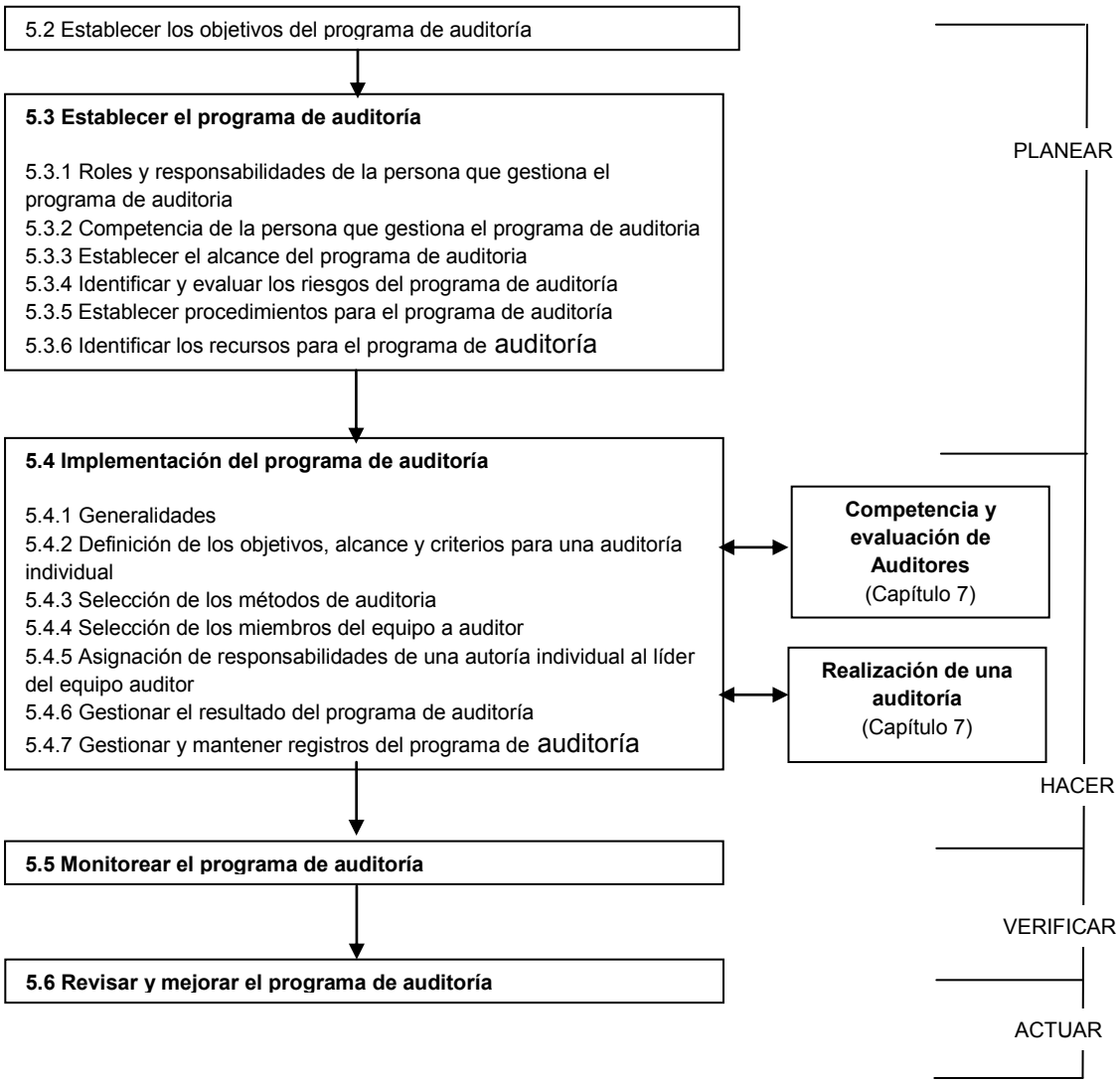
Nota 3 Cuando se auditan juntos dos o más sistemas de gestión de diferentes disciplinas (ej. calidad, ambiental, seguridad y salud ocupacional), esto se denomina auditoría combinada.

Nota 4 Cuando dos o más organizaciones cooperan para auditar a un único auditado (3.7), se denomina auditoría conjunta.

[18] OROGANIZACION INTERNACIONAL DE NORMALIZACION. Directrices para la auditoria de sistemas de gestión. ISO 19011:2011. Bogotá D.C: ICONTEC, 2011. 44p.

Nota 5 Adaptado de ISO 9000:2005, definición 3.9.1.[19]

Figura 6. Diagrama de flujo del proceso para la gestión de un programa de auditoría



Fuente: OROGANIZACION INTERNACIONAL DE NORMALIZACION. Directrices para la auditoria de sistemas de gestión. ISO 19011:2011. Bogotá D.C: ICONTEC, 2011. 44p.

[19] Ibíd., p. 44.

6. METODOLOGÍA

Este proyecto propone la metodología de elaboración de proyectos que paso a paso busca dar solución a los objetivos y actividades del proyecto, de manera ordenada y eficiente.

La metodología a desarrollar para la elaboración de este proyecto, consta en dar cumplimiento a cada uno de los objetivos definiendo las actividades necesarias para el desarrollo de los mismos.

Objetivos y actividades a desarrollar:

- Identificar el nivel de cumplimiento con respecto a las características y pilares de seguridad y privacidad de la información en la Institución

- Leer la norma ISO/IEC 27001:2013. “Sistema de gestión de seguridad de la información”.

- Leer la norma ISO/IEC 27002:2013. “Código de prácticas para la gestión de la seguridad de la información”.

- Leer ley 1581 Protección de datos personales.

- Hacer matriz con controles y dominios de la norma ISO/IEC 27002 “Código de prácticas para la gestión de la seguridad de la información” e identificar los controles que se encuentran implementados.

- Identificar los requerimientos de seguridad y privacidad de la información estipulados en la norma ISO/IEC 27001:2013 y la norma ISO/IEC 27002:2013.

- Identificar amenazas a los activos por no realizarse auditoria en seguridad de la información.

- Identificar los requisitos y controles de la Norma ISO/IEC 27002:2013 de seguridad y privacidad de la información con respecto a auditoria de seguridad de la información.

- Identificar y proponer mecanismos para el mejoramiento del procedimiento “Auditoria en Seguridad y Privacidad de la Información” de la Universidad.

- Revisar el procedimiento “Auditoria en seguridad y privacidad de la información”.

- Identificar mejoras al procedimiento “Auditoria en seguridad y privacidad de la información”.

- Proponer mecanismos para la realización de auditorías en seguridad de la información, Aplicando directrices para auditorías basándose en las normas ISO 19011:2011, ISO/IEC 27006:2011 e ISO/IEC 27007:2011.

- Diseñar el proceso para la gestión de un programa de auditoría en seguridad de la información.

  - Establecer los objetivos del programa de auditoría de seguridad de la información.

  - Establecer el programa de auditoría de seguridad de la información.

  - Implementar el programa de auditoría de seguridad de la información.

- Presentar recomendaciones sobre la implantación de medidas preventivas y correctivas al proceso de gestión de seguridad de la información.

- Identificar mejoras a los procedimientos que hacen parte del proceso Gestión de seguridad de la información.

- Presentar recomendaciones al procedimiento

- Brindar un diagnóstico a las medidas específicas de corrección.

- Elaborar análisis causa - efecto.

- Validar por medio de prueba piloto los entregables del proyecto.

- Correr mediante prueba piloto el programa de auditoría propuesto, y dar un diagnóstico sobre los hallazgos encontrados.

7. DESARROLLO

7.1 MATRIZ DE IDENTIFICACIÓN DE CONTROLES IMPLEMENTADOS

Para identificar el nivel de cumplimiento con respecto a los pilares de la seguridad y privacidad de la información, se realiza una matriz con los controles y dominios de la norma ISO/IEC 27002:2013, que se encuentran implementados. Esta matriz se hace a la coordinación de seguridad informática con los controles que aplique para esta dependencia, por ser el ente gestor de la seguridad de la información en la Universidad Autónoma de Occidente.

Tabla 2. Matriz de controles norma ISO 27001:2013 implementada

Dominio	Objetivo de Control	Control	Implementado		Comentario
			si	no	
5. Políticas de Seguridad	5.1 Directrices de la dirección en seguridad de la información	A.5.1.1 Conjunto de Políticas para la seguridad de la información	X		Fueron publicadas en el año 2013, y se revisaran cada año.
		A.5.1.2 Revisión de las políticas para la seguridad de la información	X		
12. Seguridad de Operaciones	12.4 Registro de actividad y supervisión	A.12.4.1 Registro y gestión de eventos de actividad	X		Se registra por el usuario
	12.7 Consideraciones de auditoria de sistemas de información	A.12.7.1 Controles de auditoria de los sistemas de información		X	
16. Gestión de incidentes en la seguridad de la información	16.1 Gestión de Incidentes de seguridad de la información y mejoras	A.16.1.2 Notificación de los eventos de seguridad de la información		X	
		A.16.1.3 Notificación de los puntos débiles de seguridad de la información		X	

Tabla 2. (Continuación)

16. Gestión de incidentes en la seguridad de la información	16.1 Gestión de Incidentes de seguridad de la información y mejoras	A.16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones	X		
		A.16.1.5 Respuesta a los incidentes de seguridad de la información	X		
		A.16.1.6 Aprendizaje de los incidentes de seguridad de la información		X	
		A.16.1.7 Recopilación de evidencia		X	
17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio	17. 1 Continuidad de la seguridad de la información	A.17.1.1 Planificación de la continuidad de la seguridad de la información		X	
		A.17.1.2 Implantación de la continuidad de la seguridad de la información		X	
		A.17.1.3 Verificación, revisión y evaluación de la continuidad		X	
18. Cumplimiento	18.1 Cumplimiento de los requisitos legales y contractuales	A.181.3 Protección de los registros de la organización	X		
	18.2 Revisión de la seguridad de la información	A.18.2.1 Revisión independiente de la seguridad de la información	X		

Tabla 2. (Continuación)

18. Cumplimiento	18.2 Revisión de la seguridad de la información	A.18.2.2 Cumplimiento de políticas y normas de seguridad	X		

7.2 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Se identifica las siguientes amenazas por no realizarse hoy en día auditorias de seguridad y privacidad de la información, por la falta de lineamientos para la realización de la misma.

7.2.1 Pérdida de credibilidad. Al no contar con mecanismos oficiales de auditoría en seguridad y privacidad de la información, falta evidencia de cómo se está llevando a cabo el uso de la información y de los recursos tecnológicos en la universidad, esto genera incertidumbre a colaboradores y a la alta dirección sobre el ambiente de seguridad dentro y fuera de las instalaciones del campus universitario.

7.2.2 Incumplimiento de políticas. Al no revisar el cumplimiento de las políticas de la universidad autónoma de occidente por medio de auditorías internas de seguridad y privacidad de la información, se puede perder la oportunidad de mejora de las mismas, no ver el nivel de madurez de las políticas e incluso saber la eficacia de estas para la organización.

7.2.3 Falta de registros de auditoría de seguridad y privacidad de la información. Por trazabilidad se hace necesario conservar los registros de auditora para su continuo seguimiento y mejoras de la misma, además se debería definir una forma adecuada para dar soporte a los registro de auditorías internas de la universidad, para salvaguardar la información que estas contienen logrando su mantenimiento y disponibilidad.

7.2.4 Uso inadecuado de recursos tecnológicos y de la información. A la falta de mecanismos para realizar auditorías internas de seguridad y privacidad de la información, no se tiene una evidencia de cómo se está llevando a cabo los procesos de la universidad y el cumplimiento de las políticas.

7.2.5 Problemas de administración del responsable del activo. A la falta de mecanismos para realizar auditorías internas de seguridad de la información, los responsables de activos de información no cuentan con recomendaciones y oportunas de mejoras de seguridad de la información para los activos bajo su custodia.

7.2.6 controles de la norma ISO/IEC 27001:2013 que aplican al proceso de gestión de seguridad de la información. De acuerdo a las anteriores amenazas y con respecto a realizar auditorías en seguridad y privacidad de la información se identifica los siguientes requisitos de control de la norma ISO/IEC 27001:2013 Sistema de gestión de seguridad de la información que aplican para ser implementados.

- A.5.1.2 Revisión de las políticas de seguridad de la información

Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.

- A.18.1.3 Protección de registros

Control: Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.

- A.18.2.1 Revisión independiente de seguridad de la información

Control: El enfoque de la organización para la gestión de seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para la seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.

- A.18.2.2 Cumplimiento con políticas y normas de seguridad

Control: Los directores deben revidar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.

- A.18.2.3 Revisión de cumplimientos técnico

Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

7.3 PROCEDIMIENTO "AUDITORIA EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN"

No se cuenta con el procedimiento auditoria en seguridad y privacidad de la información de manera formal para la Universidad, la coordinación de seguridad informática trabaja con documentación que se encuentra por fuera del sistema de gestión de calidad.

Actualmente se cuenta con los siguientes procedimientos para el proceso Gestión de seguridad de la información:

- DVT-3.2-PD2.1 Respuesta a eventos e incidentes de seguridad de la información
- DVT-3.2-PD2.2 Mejoras de Seguridad de la información.

De esta manera, el proyecto especifica directrices para la realización de auditorías internas de seguridad y privacidad de la información, las cuales contienen el programa de auditoría, la realización de auditorías y procedimientos para llevarlas a cabo.

Además, se recomienda formalizar el procedimiento Auditoria en seguridad y privacidad de la información, para contar con este de manera formal en el sistema de gestión de calidad de la Universidad Autónoma de Occidente.

7.4 GESTIÓN DE UN PROGRAMA DE AUDITORÍAS

Un programa de auditoría consiste en la gestión organizada y metódica de actividades que permiten llevar a cabo un número de auditorías de manera programada, es decir, la planificación de estas auditorías deben tener en cuenta un periodo de tiempo programado, número de visitas a realizar, evaluar posibles riesgos a los que se encuentra sometida, recursos necesarios, etc. Esto con el fin de contar con un programa de auditorías eficaz y eficiente dentro de lo programado; de esta forma la Universidad Autónoma de Occidente tendrá control sobre todos y cada uno de los procesos y/o actividades que lleva a cabo.

"Una organización que necesita llevar a cabo auditorias debería establecer un programa de auditoría que contribuya a la determinación de la eficacia del sistema de gestión del auditado. El programa de auditoría puede incluir auditorias que tengan en consideración una o más normas de sistema de gestión, llevadas a cabo de manera individual o combinada.

La alta dirección debería asegurarse de que los objetivos del programa de auditoría se han establecido y que se asigna una o más personas competentes para gestionar el programa de auditoría. El alcance de un programa de auditoría debería basarse en el tamaño y la naturaleza de la organización que se audita, así como en la naturaleza, funcionalidad, complejidad y nivel de madurez del sistema de gestión que se va a auditar. Debería darse prioridad a asignar los recursos del programa de auditoría para auditar los asuntos de importancia dentro del sistema de gestión. Estos pueden incluir las características clave de la calidad de un producto o los peligros relativos a la salud y la seguridad, o los aspectos ambientales significativos y su control.

El programa de auditoría debería incluir la información y los recursos necesarios para organizar y llevar a cabo sus auditorías de forma eficaz y eficiente dentro de los periodos de tiempo especificados y también puede incluir lo siguiente:

- Objetivos para el programa de auditoría y para las auditorias individuales;
- Alcance, número, tipos, duración, calendario de las auditorías;
- Procedimientos del programa de auditorías;

- Criterios de auditoría; (criterios de seguridad de la información, criterios del cliente, criterio del procedimiento)

- Métodos de auditoría;

- Selección de equipos auditores;

- Recursos necesarios, incluyendo viajes y alojamiento.

La implementación del programa de auditoría debería seguirse y medirse para asegurarse de que se han alcanzado sus objetivos. El programa de auditoría debería revisarse para identificar posibles mejoras."[20]

7.4.1 Política general de auditoria interna de seguridad y privacidad de la información. La Universidad Autónoma de Occidente consiente de la importancia de la seguridad y privacidad de la información en la comunidad universitaria y con el propósito de evidenciar el uso adecuado de la información, de los recursos tecnológicos, cumplimiento de políticas, lineamientos y procedimientos, realizara anualmente auditorías internas de seguridad y privacidad de la información, enfocando la actividad de auditoria a la mejora del proceso y concienciación del tema y así evitar eventos e incidentes de seguridad y privacidad de la información dentro del campus universitario.

7.4.2 Objetivos del programa de auditoría de seguridad de la información

- Apoyar las políticas institucionales de la Universidad Autónoma de Occidente

- Apoyar la política general de auditoria interna de seguridad y privacidad de la información

- Apoyar la política general de seguridad de la información y la política general de privacidad de la información

- Verificar el cumplimiento de la política general de seguridad de la información y la política general de privacidad de la información

- Conocer la situación actual de la seguridad y privacidad de la información de la Universidad Autónoma de Occidente

[20] Ibíd., p. 5 Y 6.

- Apoyar y contribuir con el sistema de trabajo de la Coordinación de seguridad informática "plan director de seguridad y privacidad de la información"

- Identificar los requisitos de seguridad y privacidad de la información, con respecto a los controles de la norma ISO/IEC 27001:2013

- verificación de los requisitos legales y contractuales en la universidad autónoma de occidente

- Mejorar la concienciación de la seguridad y privacidad de la información en la Universidad Autónoma de Occidente y su comunidad

7.4.3 Funciones y responsabilidades de la persona de la gestión del programa de auditoría

- Definir los procesos o áreas a ser auditadas

- Seleccionar los auditores para realizar la actividad

- Llevar la gestión del programa de auditoria interna de seguridad y privacidad de la información

- Guiar y motivar a los auditores a la realización de la actividad identificando mejoras a los procesos auditados

- Verificar el cumplimiento de las actividades programadas de la auditoria interna de seguridad y privacidad de la información

- Realizar seguimiento a los hallazgos encontrados con no conformidad para conocer el estado en que se encuentran las oportunidades de mejora de seguridad de la información

Estas directrices no van orientadas a un área o proceso en específico, el objetivo de estas, es que sirvan de guía para realizar un programa de auditorías internas teniendo en cuenta la seguridad y privacidad de la información. Por otro lado el responsable y encargado del programa de auditoría debe establecer según sea el proceso o los procesos a auditar: el alcance, objetivos, recursos, equipo auditor, evaluar riesgos, determinar cronogramas, y posterior a esto encargarse de realizar seguimiento a los hallazgos con no conformidades y a las oportunidades de mejora encontradas para conocer el estado de estas en que se encuentran.

7.4.4 Competencia de la persona responsable de la gestión del programa de auditoría. La persona encargada de la gestión del programa de auditoría en seguridad y privacidad de la información, debe tener conocimientos y competencias en el tema en cuestión.

Conocer y manejar los siguientes documentos:

- La norma ISO/IEC 27001:2013 Sistema de gestión de la seguridad de la información
- La norma ISO/IEC 27002:2013 Código de práctica para la gestión de la seguridad de la información
- La norma ISO/IEC 27007:2011 Directrices para la auditoría de sistemas de gestión de seguridad de la información
- La norma ISO 19011:2011 Directrices para la auditoria de los sistemas de gestión
- Ley 1581 de 2012 Protección de datos personales

Además conocer el funcionamiento estructural y organizacional de la universidad y generar buenas relaciones con el equipo auditor, jefe de procesos a auditar, con la alta dirección para lograr una comunicación idónea durante el proceso de auditoría interna de seguridad y privacidad de la información.

La persona responsable de la gestión del programa de auditoría debería participar en las actividades de desarrollo profesional continuo, apropiadas para mantener los conocimientos y habilidades necesarios para gestionar el programa de auditoría. [21]

7.4.5. Los auditores deberán seguir los siguientes principios de auditoría: "La auditoría se caracteriza por depender de varios principios. Estos principios deberían ayudar a hacer de la auditoria una herramienta eficaz y fiable en apoyo de las políticas y controles de gestión, proporcionando información sobre la cual una organización puede actuar para mejorar su desempeño. La adhesión a esos principios es un requisito previo para proporcionar conclusiones de la auditoria que

[21] Ibíd., p. 9.

sean pertinentes y suficientes y para permitir a los auditores, trabajando independientemente entre sí, alcanzar conclusiones similares en circunstancias similares.

- Integridad: El fundamento de la profesionalidad Los auditores y las personas que gestionan un programa de auditoría deberían:

  -Desempeñar su trabajo con honestidad, diligenciada y responsabilidad

  -observar y cumplir todos los requisitos legales aplicables

  -Demostrar su competencia al desempeñar su trabajo

  -Desempeñar su trabajo de manera imparcial, es decir, permanecer ecuánime y sin sesgo en todas sus acciones

  -Ser sensible a cualquier influencia que se pueda ejercer sobre juicio mientras lleva a cabo una auditoria

- Presentación imparcial: la obligación de informar con veracidad y exactitud. hallazgos, conclusiones e informes de la auditoria deberían reflejar con veracidad y exactitud las actividades de auditoría. Se debería informar de los obstáculos significativos encontrados durante la auditoria y de las opiniones divergentes sin resolver entre el equipo auditor y el auditado. La comunicación debería ser veraz, exacta, objetiva, oportuna, clara y completa.

- Debido cuidado profesional: la aplicación de diligencia y juicio al auditar. Los auditores deberían proceder con el debido cuidado, de acuerdo con la importancia de la tarea que desempeñan y la confianza depositada en ellos por el cliente de la auditoria y por otras partes interesadas. Un factor importante al realizar su trabajo con el debido cuidado profesional es tener la capacidad de hacer juicios razonados en todas las situaciones de la auditoria.

- Confidencialidad: Seguridad de la información.

  Los auditores deberían proceder con discreción en el uso y la protección de la información adquirida en el curso de sus tareas. La información de la auditoria no debería usarse inapropiadamente para beneficio personal del auditor o del cliente de la auditoria, o de modo que perjudique el interés

legítimo del auditado. Este concepto incluye el tratamiento apropiado de la información sensible o confidencial.

- Independencia: la base para la imparcialidad de la auditoria objetiva de las conclusiones de la auditoria.

  Los auditores deberían ser independientes de la actividad que se audita siempre que sea posible, y en todos los casos deberían actuar de una manera libre de sesgo y conflicto de intereses. Para las auditorías internas, los auditores deberían ser independientes de los responsables operativos de la función que se audita. Los auditores deberían mantener la objetividad a lo largo del proceso de auditoría para asegurarse de que los hallazgos y conclusiones de la auditoria estarán basados solo en la evidencia de la auditoria.

  Para las organizaciones pequeñas, puede que no sea posible que los auditores internos sean completamente independientes de la actividad que se audita, pero deberían hacerse todos los esfuerzos para eliminar el sesgo y fomentar la objetividad.

- Enfoque basado en la evidencia: el método racional para alcanzar conclusiones de la auditoria fiables y reproducibles en un proceso de auditoría sistemático.
  La evidencia de la auditoria debería ser verificable. En general se basara en muestras de la información disponible, ya que una auditoria se lleva a cabo durante un periodo de tiempo delimitado y con recursos finitos. Debería aplicarse un uso apropiado del muestreo, ya que está estrechamente relacionado con la confianza que puede depositarse en las conclusiones de la auditoria."[22]

7.4.6 Alcance del Programa de auditoría interna de seguridad y privacidad de la información: El alcance de una auditoria comprende la descripción de ubicaciones, procesos, dependencias, actividades a auditar. Además del establecimiento de las fechas de auditoria.

El alcance de estas directrices y programa para realizar auditorías internas de seguridad y privacidad de la información en la Universidad Autónoma de Occidente, comprende la vicerrectoria académica y vicerrectoria administrativa, es decir, cualquier proceso y/o departamento que se encuentren adscritos a estos

[22] Ibíd., p. 4 Y 5.

pueden hacer uso de estas directrices y programa para la realización de auditorías internas.

7.4.7 Identificación y evaluación de los riesgos relacionados con el programa de auditoría. La persona responsable de la gestión del programa de auditoria interna de seguridad y privacidad de la información debe tener en cuenta riesgos que puedan afectar el curso de la actividad de la auditoria, de acuerdo con esto se definen algunos riesgos que deberían ser considerados.

Riesgos:

- Los objetivos del programa de auditoría no satisfagan las necesidades de la universidad
- Que no se cumpla el cronograma de actividades de la auditoria
- Que no se cumpla el tiempo programado para elaborar la auditoria
- Falta de recursos tecnológicos para la elaboración de la auditoria
- Que el personal dispuesto a realizar la auditoria no cumpla con las competencias necesarias para el desarrollo de la misma
- Que el alcance no cumpla con el objetivo de la actividad de la auditoria
- Que el informe final de la auditoria se encuentre basado en evidencias poco fiables o no reales
- Que el programa de auditoría en seguridad y privacidad de la información, no se cumpla en su totalidad
- Que los registros de auditoría no se salvaguarden de forma adecuada
- Que no se realice seguimiento y mejoras a las directrices, programa de auditorías de seguridad y privacidad de la información.

Tabla 3. Descripción de riesgos y consecuencias

Nombre del riesgo	Descripción	Consecuencias	Medidas
Inexactitud	Los objetivos del programa de auditoría no satisfagan las necesidades de la universidad	Enfocar de manera diferente las actividades de la auditoria a lo que se tenía planeado	Corroborar la información de los objetivos con la alta dirección
Inconformidad	Que no se cumpla el cronograma de actividades de la auditoria	Obtener resultados diferentes a lo esperado	Supervisar que las actividades se lleven a cabo y que se cumpla con lo programado
Incumplimiento	Que no se cumpla el tiempo programado para elaborar la auditoria	No terminar la auditoria o pedir más tiempo para culminarla	Tener en cuenta eventos externos que no se puedan controlar al momento de elaborar el cronograma y fechas
Insuficiencia	Falta de recursos tecnológicos para la elaboración de la auditoria	Obtener resultados diferentes a lo esperado	Buscar alternativas que se adapten al presupuesto o esperar hasta tener las herramientas de trabajo
Ineficiencia	Que el personal dispuesto a realizar la auditoria no cumpla con las competencias necesarias para el desarrollo de la misma	Obtener resultados diferentes a lo esperado	Verificación de nivel de competencia y capacitación en seguridad y privacidad de la información

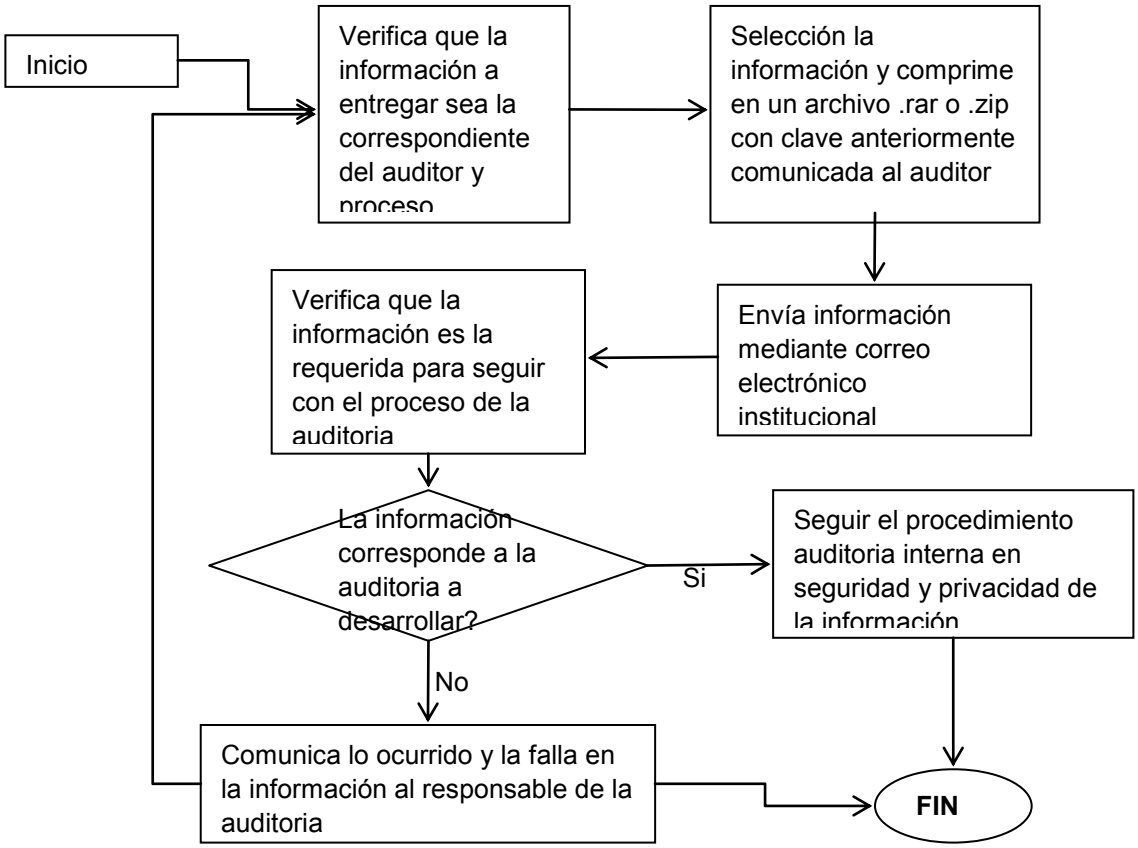
Tabla 3. (Continuación)

Evidencia poco clara	Que el informe final de la auditoria se encuentre basado en evidencias poco fiables o no reales	Obtener resultados diferentes a lo esperado, ocasionando que no se tomen las medidas necesarias para las no conformidades	el responsable del la auditoria verifique los hallazgos sustentados en pruebas reales
Incumplimiento	Que el programa de auditoría en seguridad y privacidad de la información, no se cumpla en su totalidad	No cumplir con el programa y plan de auditoría, generando inconformidad con los resultados, hallazgos y conclusiones de la auditoria.	Proponer en el programa y plan de auditorías alternativas que suplan las actividades que no se lleven a cabo, por eventos externos que no se puedan controlar (Ej: incumplimiento de alguna entrevista con el auditado por problemas de salud)
Exposición de registros de auditoria	Que los registros de auditoría no se salvaguarden de forma adecuada	No se puede hacer seguimiento a las auditorias, por falta de información.	Implementar el control de la norma ISO/IEC 27001:2013 A.18.1.3 Protección de registros
Falta de seguimiento	Que no se realice seguimiento y mejoras a las directrices, programa de auditorías de seguridad y privacidad de la información.	Pérdida de credibilidad de la seguridad de la información ante la lata dirección.	La alta dirección perciba los resultados a través de los indicadores de gestión y verificar el progreso del programa de auditoría de seguridad y privacidad de la información

Procedimientos para el programa de auditoria. El responsable de gestionar el programa de auditorías deberá instaurar procedimientos para tratar los siguientes puntos:

- Aseguramiento y entrega de información. La información debe ser comunicada por un medio de canal digital o físico, teniendo en cuenta las características de la seguridad de la información para garantizar la protección durante la manipulación de esta.

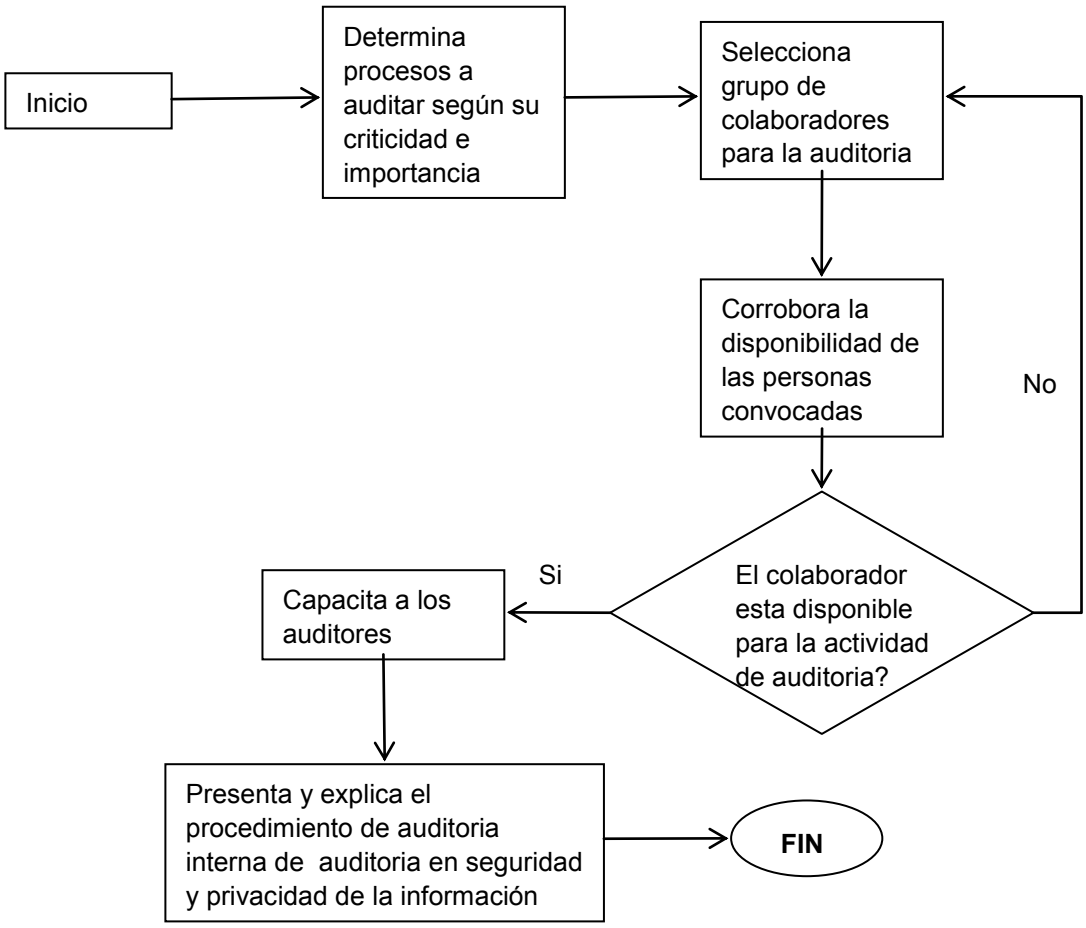
Figura 7. Procedimiento entrega de información



Fuente: Procedimiento entrega de informacion, agosto de 2014. Figura propia de la autora.

- Selección del equipo auditor y asignación de funciones y responsabilidades (Auditores internos o externos? Internos: el responsable de la gestión del programa de auditorías capacita y forma en seguridad y privacidad de la información para la auditoria, si no se cuenta con el personal capacitado dentro de la institución se contratara personal para realizar la auditoria)

Figura 8. Procedimiento selección de auditores



Fuente: Procedimiento Selección de auditores, agosto de 2014. Figura propia de la autora.

El responsable del programa de auditorías debe elegir un grupo de auditores para cubrir las auditorias que se tienen programas, a partir de esto el responsable deberá:

- Verificar las competencias de cada auditor para asignar a un proceso

- Elegir cada equipo de auditores a un proceso, evitando que un auditor pertenezca al proceso a auditar

- Elegir líder del equipo auditor
- Capacitar en seguridad y privacidad e la información a los auditores

- Orientar y motivar a los auditores a tener una comunicación amena con los auditados

- Comunicar a los auditores el programa de auditoría, metodología y formatos para realizar la actividad

El responsable del programa de auditorías debe asignar por cada equipo auditor, a un auditor líder; especificándole a este sus respectivas funciones, como: realizar el plan de auditoría, guiar al equipo que está bajo su cargo, etc. Además el responsable del programa de auditoría deberá suministrar a cada líder la información necesaria del proceso a auditar y especificar los objetivos, alcance y criterios de la auditoria en seguridad y privacidad de la información.

Para lograr una gestión eficaz y eficiente del programa de auditorías, es necesario que el responsable encargado del programa de auditorías verifique lo siguiente:

- Informes de auditoria

- Listas de verificación

- Análisis causa raíz

- Recomendaciones de oportunidades de mejora

- Hallazgos y conclusiones con información verificable

- El seguimiento a las no conformidades

7.4.2 Identificación de los recursos del programa de auditoría

- **Financieros:** Tiempo, papelería, útiles, viáticos, etc. Necesarios para las actividades de la auditoria

- **Humanos:** Auditores disponibles y capacitados en seguridad y privacidad de la información para la realización de las auditorias
- **Tecnológicos:** disponibilidad de las TIC´s

- **Infraestructura:** Instalaciones apropiadas para desarrollar las actividades de la auditoria (Evaluar posibles riesgos de infraestructura)

7.5 APLICACIÓN DEL PROGRAMA DE AUDITORIA

La persona responsable del programa de auditorías debe implementar el programa para realizarse anualmente bajo el mes o los meses que sean asignados para esta actividad a los procesos y actividades de la Universidad Autónoma de Occidente, a través de una metodología participativa y objetiva permitiendo identificar el estado actual y de cumplimiento de la seguridad y privacidad de la información en el campus universitario.

Para implementar el programa de auditorías deberá tener en cuenta lo siguiente:

- "Comunicar a las partes pertinentes del programa de auditoría a las partes correspondientes e informarlas periódicamente de su progreso.

- Definir los objetivos, el alcance y los criterios para cada auditoria individual.

- Coordinar y programar las auditorias y otras actividades relativas al programa de auditoria.

- Asegurar la selección de los equipos auditores con la competencia necesaria.

- Proporcionar los recursos necesarios para los equipos auditores.

- Asegurar la realización de las auditorias de acuerdo con el programa de auditoría y dentro del periodo de tiempo acordado.

- Asegurar que se registran las actividades de auditoría y que los registros se gestionan y mantienen adecuadamente" [23]

7.5.1 Metodología: Se pueden usar métodos in situ (en el sitio) y métodos a distancia.

Tabla 4. Métodos de auditoria

Grado de implicación entre el auditor y el auditado	**Ubicación del auditor**	
	In situ	**A distancia**
Interacción humana	Realizar entrevistas. Completar listas de verificación y cuestionarios de participación del auditado. Revisar los documentos con la participación del auditado. Muestrear	A través de medios de comunicación interactivos: -Realizar entrevistas - Completar listas de verificación y cuestionarios -revisar los documentos con la participación del auditado
Sin interacción humana	Revisar los documentos (por ejemplo, registros, análisis de datos) Observar el trabajo desempeñado. Realizar visitas al sitio. Completar listas de verificación. Muestrear (por ejemplo, productos)	Revisar los documentos (por ejemplo, registros, análisis de datos). Observar el trabajo desempeñado a través de medios de vigilancia, considerando los requisitos sociales y legales. Analizar los datos
Las actividades de auditoría in situ se realizan en las instalaciones del auditado. Las actividades de auditoría a distancia se realizan en cualquier otro lugar distinto de las instalaciones del auditado, sin tener en cuenta la distancia. Las actividades de auditoría interactivas implican la interacción entre el personal del auditado y el equipo auditor. Las actividades de auditoría no interactivas no implican la interacción humana con las personas que representan al auditado, pero implican la interacción con los equipos, las instalaciones y la documentación. De acuerdo con esto se propone lo siguiente como metodología y herramientas para realizar una auditoría en seguridad y privacidad de la información		

Fuente: OROGANIZACION INTERNACIONAL DE NORMALIZACION. Directrices para la auditoria de sistemas de gestión. ISO 19011:2011. Bogotá D.C: ICONTEC, 2011. 46 p.

[23] Ibíd., p. 12 .

- Lista de verificación

- Reunión de apertura
- Concretar y definir los auditados que se consideran imprescindibles para estar en la actividad de auditoría.

- Pactar con el responsable o jefe del proceso a auditar el día y la hora de la auditoria.

- Habrá oportunidades donde no se evidencien hallazgos o que todo esté conforme al proceso y los criterios de auditoría(es decir que no hay observaciones en la auditoria), que esta situación aporte a la identificación de oportunidades de mejora al proceso y concienciar a los auditores en no solo evidenciar lo malo sino también a contribuir a la mejora.

- Diligenciar la auditoria en el formato o lista de verificación correspondiente.

- Consultar y comprender los procedimientos, formatos, manual de funciones, indicadores de gestión y toda la documentación posible referente al proceso a auditar y a la persona auditada.

- Generar en el formato o lista de verificación preguntas concretas y claras (ser concluyente y preciso, para evitar preguntas capciosas) antes de realizar la auditoria.

- Tener en cuenta indicadores de gestión y sus resultados, registros de auditoría y seguimiento a las no conformidades, compresión del proceso, procedimientos y actividades a auditar.

- Comunicar al auditado las fallas o no conformidades encontradas en la actividad de auditoría, expresándole también que se está incumpliendo algún requisito de la norma, algún requisito del proceso o algún requisito del cliente.

- Tratar amablemente al auditado, generando un ambiente ameno para desarrollar la actividad (Que este no sienta que se está sometiendo a un juicio para ser condenado).

7.5.2 Gestión y mantenimiento de los registros del programa de auditoría. El responsable del programa de auditorías debe salvaguardar los registros de auditoría teniendo en cuenta los tres pilares de la seguridad de la información (Integridad, disponibilidad y confidencialidad), para garantizar que se mantienen los registros de auditoría.

Los registros deberán contener:

Registros relacionados con el programa de auditoría (objetivos, alcance, riesgos, y revisiones de la eficacia del programa de auditorías).

Registros relacionados con cada auditoria individual (plan de auditoría, Informes de auditoría, no conformidades, acciones correctivas y preventivas, seguimiento a las no conformidades).

Registros relacionados con el personal de auditoría (selección de auditores, competencias, desempeño durante la actividad).

7.5.3 Seguimiento, revisión y mejora del programa de auditoría interna de seguridad y privacidad de la información. El responsable de la gestión del programa de auditorías deberá identificar el progreso y la contribución del programa de gestión de auditorías en seguridad y privacidad de la información a la universidad, verificando lo siguiente:

- Cuantas acciones correctivas y preventivas han dejado las no conformidades y hallazgos encontrados en cada auditoria.

- Cuantas auditorias se han realizado para verificar la seguridad y privacidad de la información en los procesos de la Universidad Autónoma de Occidente, a partir del programa de auditorías

- Evaluar el desempeño de los auditores y tiempo de realización de la actividad.

- El responsable del programa de auditorías para medir los anteriores parámetros puede definir indicadores de gestión, que además sirvan para la retroalimentación y mejora del programa.

Se propone los siguientes indicadores de gestión:

$$\text{Eficacia} = \frac{\text{Numero de auditorias realizadas anualmente}}{\text{Numero de auditorias programas anualmente}}$$

$$\text{Eficiencia} = \frac{\text{Tiempo usado en las auditorias}}{\text{Tiempo programado}}$$

$$\text{Efectividad} = \frac{\text{Numero de acciones correctivas aplicadas}}{\text{Numero de acciones correctivas detectadas}}$$

$$\text{Mejora} = \frac{\text{Numero de mejoras implementadas}}{\text{Numero de mejoras encontradas}}$$

Se debe comunicar a la alta dirección los resultados obtenidos de la gestión del programa de auditorías como informar los cambios o mejoras que se den a partir de estos resultados.

7.5 REALIZACIÓN DE UNA AUDITORIA EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Tabla 5. Descripción de las actividades de auditoria interna de seguridad y privacidad de la información

Descripción de las actividades de auditoria	
Actividad	Descripción
Elaborar el programa de auditorias	Se elabora el programa de auditoría interna de seguridad y privacidad de la información anualmente, siguiendo las directrices de auditorías de la norma ISO/IEC:27007:2013 y la norma ISO 19011:2012, generando las mejoras correspondiente al programa de acuerdo a los indicadores de gestión y resultados de auditorías anteriores; además se informa a la alta dirección la necesidad e importancia de llevar a cabo el proceso de auditoría, especificando objetivos, alcance, metodología, etc.
Elabora plan de auditoria	La persona responsable de la auditoria asigna en cada equipo auditor un líder, quien deberá diligenciar el plan de auditoría. El documento plan de auditoría debe ser entregado al responsable de la auditoria y al responsable del proceso a auditar, para la autorización de este.

Tabla 5(Continuación)

Prepara auditoria	Si el plan de auditoría no es autorizado por inconformidad en el documento, no hay disponibilidad de recursos, o algún otro motivo, se debe, buscar, corregir o proponer otra alternativa para llegar a un acuerdo en común (modificación del documento, proponer nueva fecha, etc) Si el plan de auditoría es autorizado: -Se debe verificar la información que esta sea pertinente a la auditoria, es decir, que la información este completa, es correcta, coherente y actualizada. -Se evalúa la información de acuerdo a los objetivos, procedimientos, servicios, funciones, auditorias anteriores, criterios de auditoría. -Se prepara los documentos de trabajo en el formato de auditoria o lista de verificación para registrar las observaciones, oportunidades de mejora y los hallazgos con no conformidades.
Realización de reunión de apertura	Esta reunión se hace con las personas involucradas en la auditoria, con el propósito de: -Revisar el plan de auditoría y confirmar el acuerdo entre ambas partes. -Presentar el grupo auditor -Indicar como se realizaran las actividades y como están planificadas -Establecer canales de comunicación -Acordar la fecha y hora de reunión de cierre Además se debe dar un espacio de tiempo para la formulación de preguntas.
Revisión de documentación	Los auditores deben revisar la documentación con la que cuenta para la identificación de los criterios de seguridad y privacidad de la información a revisar durante la actividad de auditoria, además identificar si hace falta documentación para lograr el objetivo de la actividad.
Establecer comunicación	El responsable de la gestión del programa de auditoria interna de seguridad y privacidad de la información debe establecer un canal de comunicación con el equipo auditor para estar en contacto, además de establecer reuniones con el equipo de trabajo para interactuar y verificar como está fluyendo la actividad, inconvenientes y progreso de la misma.
Recolección y verificación de información	

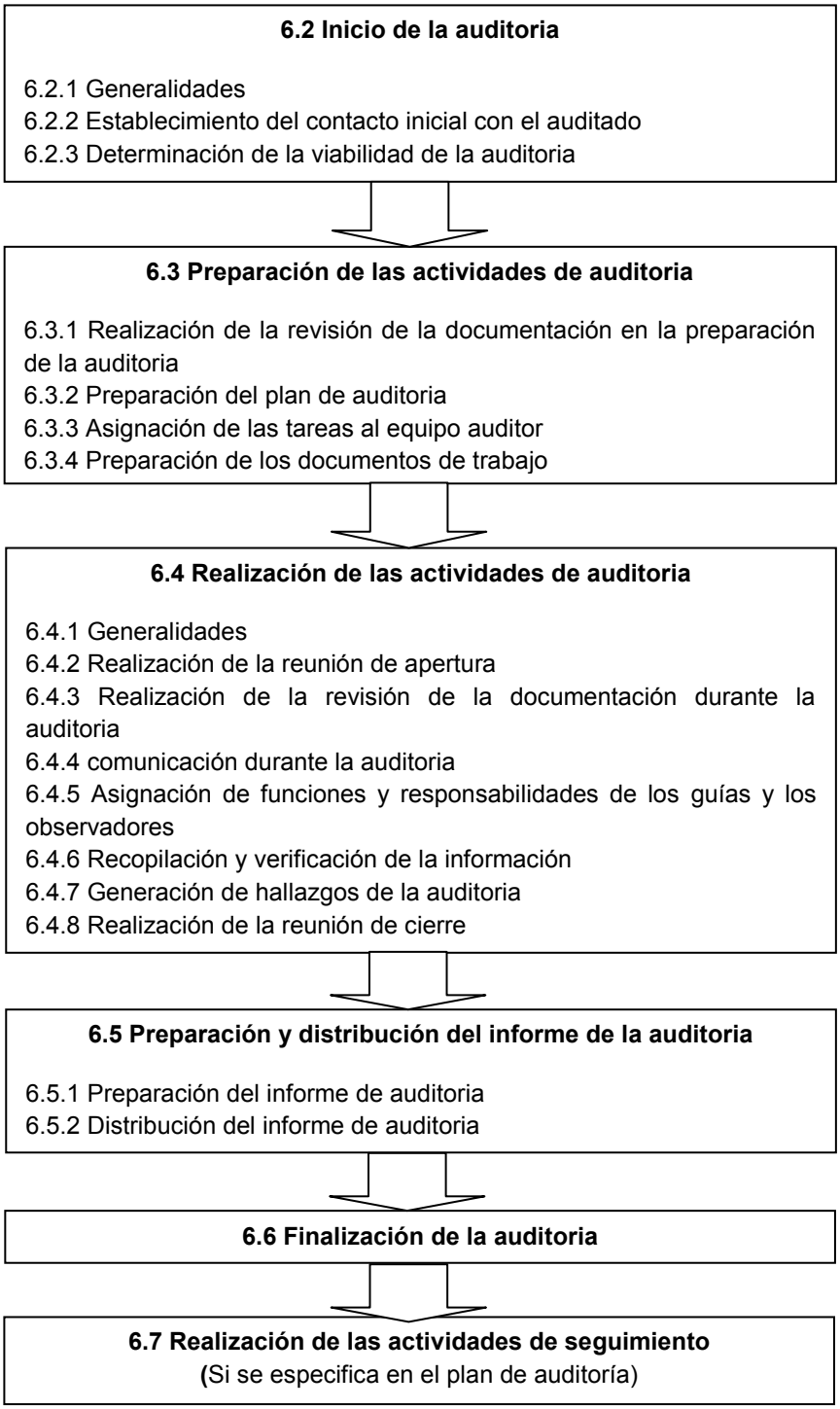
Tabla 5. (Continuación)

	Se debe revisar y comprender la documentación del auditado (procesos, procedimientos, manual de funciones, indicadores de gestión, etc). Durante la auditoria la recopilación de información se puede obtener de varias fuentes, -Entrevistas -Revisión de documentos -Registro de base de datos -Evaluación de desempeño e indicadores de gestión -Revisión de registros de auditorías anteriores.
Hallazgos y conclusiones de auditoria	Se debe evaluar la información recolectada frete a los criterios de auditoría que hayan sido formulados. El equipo auditor se debe reunir para acordar las conclusiones y recomendaciones a los hallazgos encontrados como conformidades o no conformidades.
Reunión de cierre	Esta reunión se realiza con el responsable de la auditoria, el líder del equipo auditor, responsable del proceso auditado y el auditado si es necesario; para presentar los hallazgos, observaciones, no conformidades, oportunidades de mejora encontradas y conclusiones. Además se informa la fecha sobre el seguimiento a las no conformidades y recomendaciones de oportunidades de mejora encontradas.
Preparación del informe	El líder del equipo auditor deberá elaborar el informe de la auditoria, especificando el proceso auditado, auditores, alcance, fecha, responsable de la auditoria, los hallazgos con no conformidades, oportunidades de mejora y conclusiones; además el informe deberá ser presentado en la fecha acordada al responsable del proceso auditado, responsable de la auditoria y a la alta dirección.
Fin de la auditoria	La auditoría termina cuando se haya culminado las actividades programas de la auditoria interna de seguridad y privacidad de la información. El responsable del programa deberá tomar las lecciones aprendidas de la actividad para la mejora continua de la gestión de auditorías siguientes.
Seguimiento de hallazgos	El responsable de la gestión del programa de auditoria interna de seguridad y privacidad de la información deberá realizar el seguimiento a las acciones correctivas y preventivas que se recomendaron implementar de acuerdo a los hallazgos encontrados en la actividad, para verificar el cumplimiento o el estado en que se encuentren las recomendaciones.
Fin del ciclo	Se informa a la alta dirección los resultados obtenidos de la actividad, el estado de las acciones correctivas y acciones preventivas identificadas en la actividad.

Para la realización de la gestión del programa de auditorías se definen los siguientes procedimientos y formatos:

- Procedimiento auditoria interna de seguridad y privacidad de la información
- Procedimiento selección de auditores
- Procedimiento entrega de información
- Formato plan de auditoria
- Formato lista de verificación
- Formato informe de auditoria

Figura 9. Actividades típicas de la auditoria



Fuente: OROGANIZACION INTERNACIONAL DE NORMALIZACION. Directrices para la auditoria de sistemas de gestión. ISO 19011:2011. Bogotá D.C: ICONTEC, 2011. 18 p.

7.5.2 Criterios para la auditoria.

Criterio de seguridad de la información: Verificar el cumplimiento del proceso a auditar y procedimientos con respecto a los pilares de la seguridad de la información (integridad, disponibilidad y confidencialidad), teniendo como base guía los controles de la norma ISO/IEC 27001:2013.

Criterio de procedimiento: Verificar el cumplimiento de las actividades del auditado su procedimiento y verificar que este realice las actividades que se le indican en el procedimiento y manual de funciones, con respecto a la seguridad de la información.

Criterio del usuario: verificación de los requisitos legales con respecto al cumplimiento de ley, ley 1581 de 2012 protección de datos personales.

7.5.3 Normas para realizar auditoria en seguridad y privacidad del a información

- Competencias profesionales como auditor, tener experiencia como auditor, habilidad para comunicarse, conocimiento de métodos y herramientas para auditar, manejo de procesos y procedimientos.

- Evitar reaccionar a comentarios negativos hechos por el auditado.

- Preparación del ambiente para la entrevista de auditoria, la auditoria debe realizarse en el sitio donde se lleva a cabo la actividad o proceso a auditar, con el fin de realizar o demostrar cómo se sigue el procedimiento del auditado, siempre y cuando se necesite.

- Fijar un tiempo a la entrevista de la auditoria, e informarle al auditado cuanto tiempo va a tomar el desarrollo de la actividad.

- El auditor debe mantener una actitud independiente y objetiva para la elaboración de la auditoria.

- En caso de que sea un auditor interno, evitar que este realice actividades de auditoria en procesos donde tiene o tuvo responsabilidades.

- Los auditores deben mantener absoluta reserva de la información de la auditoria, como el desempeño y resultados de la actividad, esto aun después de haber culminado la actividad.

- Los auditores solo harán las funciones delegadas a su actividad de auditoria en seguridad y privacidad de la información, no ejercerán ninguna labor distinta a esta.

- Obtención de la evidencia suficiente, competente y pertinente; esto a través de las herramientas de trabajo.

- Elaborar programa de auditorías en seguridad y privacidad de la información

7.6 ANÁLISIS CAUSA Y EFECTO:

Tabla 6. Análisis causa y efecto.

Causa	Efecto
No hay lineamientos y directrices para hacer auditorias en seguridad de la información en la universidad.	Falta de la identificación del buen uso de la información y de los recursos tecnológicos
	Genera incertidumbre a la alta dirección de la gestión de la seguridad y privacidad de la información
	Incumplimiento de políticas de seguridad y privacidad de la información
	Uso inadecuado de la información
	Uso inadecuado de los recursos tecnológicos
	Problemas de administración del responsable del activo
	Falta de conocimiento de la seguridad y privacidad de la información en los procesos de la universidad
	Ocurrencia de eventos e incidentes de seguridad de la información
	Resultados diferentes a lo esperado en la auditorias de seguridad y privacidad de la información

8 CONCLUSIONES

- Una auditoria de seguridad y privacidad de la información es la revisión y verificación al cumplimiento de lineamientos, políticas, procesos, controles, buen uso de los recursos tecnológicos y de la información; para identificar así mejoras de seguridad de la información y posibles riesgos.

- Al proyecto se le proponen tres criterios para realizar la auditoria interna de seguridad y privacidad de la información, verificación a controles de seguridad implementados (ISO/IEC 27001:2013), verificación al cumplimiento de ley (LEY 1851 de 2012) y verificación del proceso para mejoras de seguridad de la información.

- Los resultados de una auditoria en seguridad y privacidad de la información ayudan a la toma de medidas preventivas y/o correctivas evitando la ocurrencia de eventos e incidentes de seguridad de la información.

- La prueba piloto realizada para el proyecto no será presentada en el documento escrito, debido al contenido que esta tiene, la Universidad Autónoma de Occidente sostiene que es información netamente confidencial por ende se evita a ser expuesta a terceros.

- En la prueba piloto surgieron mejoras de seguridad y privacidad de la información para el proceso auditado y al proceso de gestión de seguridad de la información, al evidenciar que no se tenía en cuenta ciertos aspectos, que evaluaran si es necesario asumir e implementar las mejoras encontradas.

- De la familia de normas para la seguridad de la información ISO 27000, se encuentra La norma ISO/IEC 27007:2011 Directrices para la auditoría de sistemas de gestión de seguridad de la información, no obstante se usó como guía base la norma ISO 19011:2011 Directrices para la auditoría de sistemas de gestión, porque la actividad de auditoria se propone realizar a los procesos de la Universidad y no a un Sistema de Gestión de seguridad de la información.

- Muchas de las grandes organizaciones hoy en día le han dado la importancia prioritaria a sus activos de información, tomando medidas para la mitigación de riesgos de seguridad y privacidad de la información, sin embargo algunas

organizaciones no hacen revisión del funcionamiento y eficacia a estos controles implementados.

- Al realizar auditorías internas de seguridad y privacidad de la información, se puede aprovechar la actividad para orientar y dar tips al buen uso de la información y de los recursos tecnológicos en el entorno profesional y personal. Generando para la Universidad un valor agregado, conocimiento en el tema de seguridad y privacidad de la información en la comunidad universitaria.

9 RECOMENDACIONES

- Realizar el programa de auditoria interna de seguridad y privacidad de la información teniendo en cuenta los lineamientos y directrices para su desarrollo.

- Para empezar con el proceso de auditoría interna de seguridad y privacidad de la información, se recomienda orientar a los auditores llevar la actividad a la concienciación del tema de seguridad de la información, brindando tips y recomendaciones.

- Tomar en cuenta los riesgos a los que puede estar expuesta la actividad de la auditoria para la elaboración de las actividades y cronogramas.

- Para la selección de los procesos a auditar se recomienda hacer valoración de activos para empezar a tener en cuenta los activos de mayor criticidad para la universidad y dar prioridad a estos.

- Seleccionar auditores internos, capacitar a colabores en seguridad y privacidad de la información, evitando contratar personal capacitado y generando mayor conocimiento en el tema de seguridad en la universidad.

- Realizar seguimiento a la gestión del programa de auditoria interna de seguridad y privacidad de la información anualmente para evidenciar el progreso y contribución a la Universidad Autónoma de Occidente.

BIBLIOGRAFÍA

Concepto de Seguridad Informática Empresa Yumbo ESPY, [en línea]. [Consultado el 10 Junio del 2013]. Disponible en Internet: http://www.espyumbo.com/portalespy/index.php?option=com_content&view=article&id=78:segu

Contenido sobre la ISO 27000, [en línea]. [Consultado el 13 de Octubre del 2013]. Disponible en Internet: http://www.iso27000.es/download/doc_iso27000_all.pdf.

Controles ISO/IEC 27002: 2005, ISO, [en línea]. [Consultado el 05 de Julio del 2013]. Disponible en Internet: http://www.iso27000.es/download/ControlesISO27002-2005.pdf.

Estándar de Seguridad de la Información, Security Advisor, [en línea]. [Consultado el 05 de Julio del 2013]. Disponible en Internet: http://www.gcpglobal.com/docs/Intro_ISO27001.pdf.

Estándares y Normas de Seguridad, Familia de la Norma ISO/IEC 27000, [en línea]. [Consultado el 05 de Julio del 2013]. Disponible en Internet: http://ccia.ei.uvigo.es/docencia/SSI/normas-leyes.pdf.

GOMEZ, ÁLVARO, Enciclopedia de la Seguridad Informática, Segunda Edición, Mexico; RA-MA EDITORIAL, 2011. 367p.

VILLALÓN, HUERTA, Antonio. Códigos de buenas prácticas de seguridad UNE-ISO/IEC 17799 [en línea]. España, 2004 [consultado el 13 de Octubre del 2013]. Disponible en Internet: http://www.shutdown.es/ISO17799.pdf

Anexos

Anexo A. Procedimiento

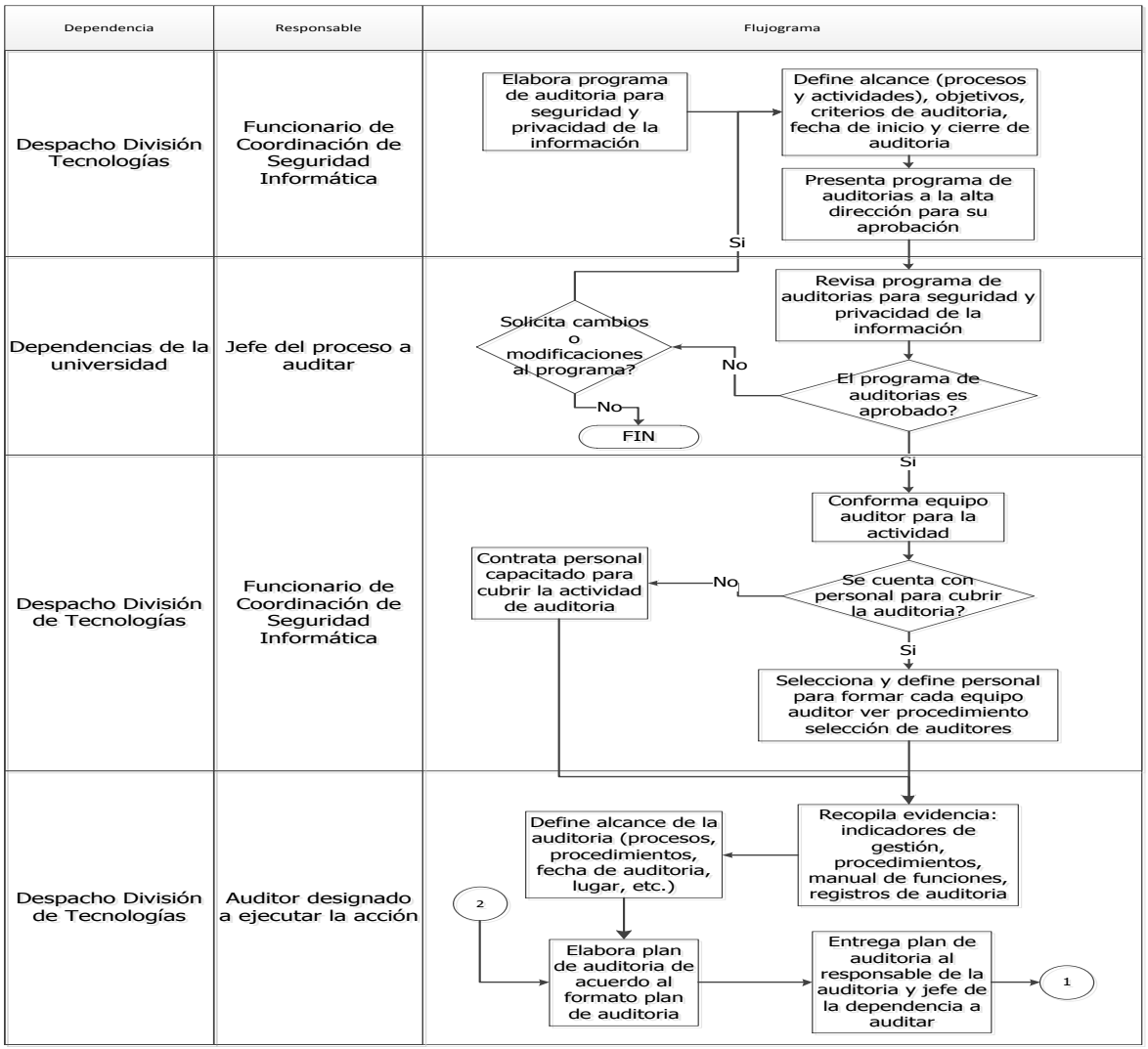
Vicerrectoría Administrativa y Financiera
División de Tecnologías

UNIVERSIDAD AUTÓNOMA DE OCCIDENTE
COPIA NO CONTROLADA
Departamento de Evaluación Organización Y Métodos

Universidad AUTÓNOMA de Occidente

do	
alizado	

PROCEDIMIENTO
Auditoria de seguridad y privacidad de la información



PROCEDIMIENTO
Auditoria de seguridad y privacidad de la información

Dependencia	Responsable	Flujograma
Despacho División Tecnologías	Funcionario de Coordinación de Seguridad Informática	1 → Revisa plan de auditoria de seguridad y privacidad de la información → Solicita cambios al plan de auditoria? Si → 2 / No
Despacho División Tecnologías	Auditor designado a ejecutar la acción	Envía plan de auditoria, agenda de auditoria, además solicita el nombre y los cargos de los funcionarios que intervendrían en la actividad de auditoria
Dependencias de la Universidad	Jefe Dependencia a auditar	Revisa agenda y plan de auditoria de seguridad y privacidad de la información → Solicita cambios al plan de auditoria? Si → 2 / No
Despacho División Tecnologías	Auditor asignado a ejecutar la acción	Invita a los auditados a reunión de apertura → Elabora lista de verificación → Realiza entrevistas, recolección y verificación de documentos, información y evidencia de hallazgos, entre otros → Diligencia en el formato de lista de verificación las observaciones y resultados de la entrevista → Verifica y valora la información de acuerdo a los criterios de la auditoria en seguridad y privacidad de la información
Dependencias de la Universidad	Auditores y auditados	El auditor invita a los auditados a la reunión de cierre, para presentar los hallazgos, no conformidades y conclusiones de la auditoria → 3

PROCEDIMIENTO
Auditoria de seguridad y privacidad de la información

Dependencia	Responsable	Flujograma
Despacho División Tecnologías	Auditor líder designado a ejecutar la acción	3 → Elabora informe final de la auditoria diligenciándolo en el formato correspondiente (informe de auditoria) → Entrega informe final al responsable de la auditoria, anexando todo el material de trabajo de la auditoria(lista de verificación, plan de auditoria, etc) → Sociabiliza y entrega el informe final con fecha de cumplimiento a las recomendaciones de las acciones correctivas y preventivas al jefe de la dependencia auditada, para el respectivo seguimiento → Realiza seguimiento al cumplimiento de las acciones correctivas y preventivas tomadas por el auditado → Realiza informe comunicando los resultados del seguimiento de la auditoria → Sociabiliza el informe de seguimiento de auditoria al jefe de la dependencia auditada
Despacho División Tecnologías	Funcionario de Coordinación de Seguridad Informática	Valida los resultados del programa de auditoria, por medio de los indicadores de gestión del programa → Realiza informe comunicando los resultados de los indicadores de gestión y las conclusiones que deja la actividad de auditoria interna en seguridad y privacidad de la información → Sociabiliza el informe con la alta dirección → FIN

Anexo B. Formato plan de auditoría.

Vicerrectoría Administrativa y Financiera
División de Tecnologías

PLAN DE AUDITORIA
Auditoria de seguridad y privacidad de la información

Proceso	
Dependencia del proceso	
Responsable del proceso	
Auditado(s)	
Objetivos de la auditoria	
Alcance de la auditoria	
Criterios de la auditoria	
Fecha de la auditoria	
Documentos de referencia	

Declaración de Confidencialidad:
Toda información suministrada y manipula durante el proceso de esta auditoría será de carácter confidencial, es decir que no podrá ser expuesta a terceros o personas que no hagan parte del proceso de esta auditoría, aun después de haber culminado la actividad.
Cordialmente,

_____
Auditor.

Anexo C. Formato Lista de verificación.

Vicerrectoría Administrativa y Financiera
División de Tecnologías

UNIVERSIDAD AUTÓNOMA DE OCCIDENTE
COPIA NO CONTROLADA
Departamento de Evaluación Organización Y Métodos

Universidad AUTÓNOMA de Occidente

LISTA DE VERIFICACION
Auditoria de seguridad y privacidad de la información

Proceso:
Dependencia del proceso:
Auditado:
Fecha:

Requisito o control del la norma ISO/IEC 27001:2013	Pregunta	Evidencia	Observación

Anexo D. Formato Informe de auditoría.

Vicerrectoría Administrativa y Financiera
División de Tecnologías

UNIVERSIDAD AUTÓNOMA DE OCCIDENTE
COPIA NO CONTROLADA
Departamento de Evaluación Organización Y Métodos

Universidad AUTÓNOMA de Occidente

INFORME DE AUDITORIA
Auditoria de seguridad y privacidad de la información

Proceso:

Dependencia del proceso:

Fecha:

Alcance:

Auditados:

Auditor(es):

Control de la norma ISO/IEC 27001:2013	Hallazgo de no conformidad	Recomendación

Control de la norma ISO/IEC 27001:2013	Oportunidad de mejora

Conclusiones de la auditoria

-

Auditores:

_____ _____